PAT-NO: JP02000216774A

DOCUMENT-IDENTIFIER: JP 2000216774 A

TITLE: CIPHER TEXT VERIFYING METHOD, RECORDING MEDIUM AND DEVICE THEREOF

PUBN-DATE: August 4, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
ABE, MASAYUKI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NIPPON TELEGR & TELEPH CORP	N/A

APPL-NO: JP11015409

APPL-DATE: January 25, 1999

INT-CL (IPC): H04L009/32 , G09C001/00

ABSTRACT:

PROBLEM TO BE SOLVED: To verify the propriety of a cipher text without absolutely leaking information about a value in a verification expression by exponentiating a value calculated for verification, when **Cramer-Shoup** cryptograph is decoded by random numbers whose values are incapable for anyone to know trying to decode it and verifying whether or not the exponentiated result becomes 1.

SOLUTION: Although a cipher text prepared by a cipher text preparing device 11 is decoded by the device 12 of a decoding person, a device 13 of a verifying person verifies whether or not decoding rejection is appropriate so as to avoid rejecting decoding, because it is not a correct cipher text in a self-serving manner. After receiving a cipher text E=(u1, u2, v, e) of a plaintext (m) enciphered by the **Cramer-Shoup** cryptograph method making X, Y and Z

public keys, the device 12 generates a random number (r) and calculates (c)=H (u1, u2) and (v)=(u1X1+CY1u2X2+CY2V1)r mod (p). If (v) is 1, this cipher text is deemed accepted, but if (v) is not 1, it is deemed rejected, and the rejection is verified to a third person.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216774

(43)Date of publication of application : 04.08.2000

(51)Int.Cl. H04L 9/32
G09C 1/00

(21)Application number : 11-015409

(22)Date of filing : 25.01.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(72)Inventor : ABE MASAYUKI

(54) CIPHER TEXT VERIFYING METHOD, RECORDING MEDIUM AND DEVICE THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To verify the propriety of a cipher text without absolutely leaking information about a value in a verification expression by exponentiating a value calculated for verification, when Cramer-Shoup cryptograph is decoded by random numbers whose values are incapable for anyone to know trying to decode it and verifying whether or not the exponentiated result becomes 1.

SOLUTION: Although a cipher text prepared by a cipher text preparing device 11 is decoded by the device 12 of a decoding person, a device 13 of a verifying person verifies whether or not decoding rejection is appropriate so as to avoid rejecting decoding, because it is not a correct cipher text in a self-serving manner. After receiving a cipher text E=(u1, u2, v, e) of a plaintext (m) enciphered by the Cramer-Shoup cryptograph method making X, Y and Z public keys, the device 12 generates a random number (r) and calculates (c)=H (u1, u2) and (v)= (u1X1+CY1u2X2+CY2V1)r mod (p). If (v) is 1, this cipher text is deemed accepted, but if (v) is not 1, it is deemed rejected, and the rejection is verified to a third person.

LEGAL STATUS

[Date of request for examination]	26.12.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3302335
[Date of registration]	26.04.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

Claim(s)]
Claim 1] The cipher verification approach characterized by verifying a cipher by checking whether the value which generated the random number r and squared the value V of an original verification type r in the cipher verification approach verified by checking that the received cipher is made justly and that the value of a verification type is set to 1 is set to 1.
[Claim 2] Considering as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, Gq is multiplicative-group Zp*. The subgroup of order q shall be expressed. g1 and g2 A logarithm considers as the origin of strange Gq and H is made into a general-purpose Hash Function. dispersion of g2 which uses g1 as a bottom -- (x1, x2, y1, y2, z) **Zq5 A private key, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) are used as a public key. In the code approach to include the cipher E over Plaintext m -- c -- as H(u1, u2) mod q -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p -- three -- constructing (u1, u2, v) -- Decode person equipment is the cipher verification approach characterized by verifying the justification of a cipher by generating a random number r, calculating c=H(u1, u2) mod q, calculating V=(u1x1+cy1u2 x2+cy2v-1) r mod p, and checking that V is equal to 1.
[Claim 3] The cipher verification approach characterized by proving that it is the result of V calculating like r mod p (u1x1+cy1u2 x2+cy2v-1) in the cipher verification approach of claim 2 to the random number r which uses zero information certification when not equal to 1, and has V to a third party.
[Claim 4] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. Make g1 and g2 into the origin of Gq, make H into a general-purpose Hash Function, and n persons' decode person is set to P1-Pn. Each decode person Pj has the open value wj of a proper, and is **(x1, x2, y1, y2, z) Zq5. Distribute with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. The secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj is used as the decode person's Pj private key. Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) are used as the decode person's Pj public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. The decode person Pj shall hold the secrecy value rj corresponding to a value wj which distributes random-number r**Zq with the secrecy variational method of threshold t, and is acquired. E= (u1, u2, v, e) is made into the cipher of the plaintext m which used 1x1g 2 x2modp of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p as the public key. When a right cipher satisfies u1=g1r mod p, u2=g2r mod p, c=H (u1, u2), v=Xr Ycrmod p, and e=mZr mod p, The equipment of each decode person Pj who received E calculates c=H (u1, u2). Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p is calculated. Distribute Vj with a verifiable secrecy variational method 2t or less more than threshold t, and are obtained. The equipment of the decode person Pk who transmitted the secrecy value Vjk corresponding to a value wk through the channel safe for each decode person's Pk equipment, and received Vjk from all other decode person equipments Vkj to which the equipment of each decode person Pj who transmitted Vk to all other decode person equipments, and received Vk corresponds according to a broadcast mold channel is transmitted to all other decode person equipments according to a broadcast mold channel. Each decode person equipment is verified using all Vkj(s) to which each Vk received that it was a right value. Choose 2t+1 piece among the right and checked Vk, and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1. If equal and a restoration value is [a secrecy restoration procedure is similarly repeated in other 2t+1 piece combination and] all equal to 1 about no combination The cipher verification approach characterized by judging that the cipher is inaccurate, and judging the cipher to be the right if there is combination set to 1 at least one.
[Claim 5] In the cipher verification approach of claim 4, if the above-mentioned cipher is judged to be the right, w will be used as the n-th root of 1 in mod q. Each decode person equipment Set wj to wj-1 mod q and it considers as the characteristic value of disclosure of wj which fills wj!=1 in 1<j<n. the dispersion which each decode person's Pj equipment calculates Dj=u1zjmod p, transmits it to all other decode person equipments according to a broadcast mold channel, and uses as a bottom u1 which received (D1, --, Dn) -- the cipher verification approach characterized by checking that a logarithm is the codeword of a BCH code.
[Claim 6] Considering as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, Gq is multiplicative-group Zp*. The subgroup of order q shall be expressed. g1 and g2 A logarithm considers as the origin of strange Gq and H is made into a general-purpose Hash Function. dispersion of g2 which uses g1 as a bottom -- (x1, x2, y1, y2, z) **Zq5 A private key, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) are used as a public key. In the code approach to include the cipher E over Plaintext m -- c -- as H(u1, u2) mod q -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p -- three -- constructing (u1, u2, v) -- Decode person equipment generates a random number r, and calculates x1'=x1 and rmod q, x2'=x2 and rmod q, y1'=y1 and rmod q, and y2'=y2 and rmod q. The cipher verification approach characterized by verifying the justification of a cipher by calculating c=H(u1, u2) mod q, calculating V=u1x1'+cy1' u2 x2'+cy2' v-rmod p, and checking that V is equal to 1 from the received cipher.
[Claim 7] In the cipher verification approach of claim 6 when not equal to 1, V decode person equipment (X, Y, V) It receives that it is (x1, x2, y1, y2, r). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and V=u1x1r+cy1r u2x2r+cy2r satisfying v-rmod p -- zero information certification -- using (x1, x2, y1, y2), considering as secrecy The cipher verification approach characterized by what is proved to a verification person.
[Claim 8] It is under Gq whose logarithm is strange. dispersion of h to which g and h use g as a bottom in the cipher verification approach of

laim 7 -- decode person equipment Random numbers r, a1, a2, b1, and b2 are generated. R=gr ha mod p, RX1=Rx1ha1mod p, :X2=Rx2ha2mod p, R, RX1, RX2, RY1, and RY2 are exhibited. RY1=Ry1hb1mod p and RY2=Ry2hb2mod p -- (X, Y, V, R, RX1, RX2, :Y1, RY2) receive that it is (x1, x2, y1, y2, r, a, a1, a2, b1, b2). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, V=u1x1r+cy1r u2x2r+cy2r v- mod p, R=gr ha mod p, RX1=Rx1ha1mod p, RX2=Rx2ha2mod p, RY1=Ry1hb1mod p, and RY2=Ry2hb2mod p -- the cipher verification :pproach characterized by proving filling relational expression by zero information certification.
Claim 9] n persons' decode person is set to P1-Pn in the cipher verification approach of claim 6. Use w as the n-th root of 1 in mod q, and wj is et to wj-1 mod q. wj!=1 shall be filled in 1<j<n and a value wj is assigned to each decode person Pj. The decode person's Pj private key (x2 j :nd y1 j, y2 x1j, j, zj) Distribute x1, x2, and (y1, y2, z) with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. :onsider as the secrecy value corresponding to a value wj, and Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1Zjmod p (Xj, Yj, Zj) :re used as the decode person's Pj public key. A safe channel shall be between each decode person equipment. Moreover, each decode person :quipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. :he decode person Pj shall hold the secrecy value rj corresponding to a value wj which distributes random-number r**Zq with the secrecy :ariational method of threshold t, and is acquired. Each decode person's Pj equipment Distribute r-x1, r and x2, r-y1, and r-y2 with the secrecy :ariational method of threshold t, respectively, and are obtained. The equipment of each decode person Pj who calculated and held secrecy :alue x1j' corresponding to a value wj, x2j', y1j', and y2j' by the distributed multiplication method, and received the cipher c=H (u1, u2) is :alculated and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p is calculated. According to a broadcast mold channel Transmit Vj to all other decode)erson equipments, and it checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code. The cipher verification approach :haracterized by verifying the justification of a cipher by checking that the value V restored with the secrecy restoration procedure to exponent)art is equal to 1.
Claim 10] In the cipher verification approach of claim 9, 2t<n shall be filled for threshold t. Instead of checking that the exponent part of (V1, --, Vn) is the codeword of a BCH code Each decode person's Pj equipment without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / right count, and] x1j', x2j', y1j', y2j', and rj The cipher verification approach characterized by)roving to other decode person equipments, specifying the decode person Pj in whom zero information certification failed as a deviation)erson, and other decode person equipments restoring a deviation person's secrecy value x1j', x2j', y1j', y2j', and rj using secrecy value :ecovery procedure by zero information certification.
Claim 11] When (V1, --, Vn) are not the codewords of a BCH code, in the cipher verification approach of claim 9 each decode person's Pj :quipment Without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', :1j', y2j', and rj Prove to other decode person equipments by zero information certification, and the equipment of the decode person Pj who :ailed in certification is specified with a deviation person's equipment. The cipher verification approach characterized by other decode person :quipments restoring secrecy value x1j' of a deviation person's equipment, x2j', y1j', y2j', and rj using secrecy value recovery procedure.
Claim 12] the dispersion each decode person's Pj equipment calculates Dj=u1zjmod p, and whose value V which carried out [above- :nentioned] restoration transmits to all other decode person equipments according to a broadcast mold channel, and uses as a bottom u1 which :eceived (D1, --, Dn) in the cipher verification approach of claim 9 when equal to 1 -- the cipher verification approach characterized by to :heck that a logarithm is the codeword of a BCH code.
[Claim 13] The restored value V in the cipher verification approach of claim 10 when equal to 1 Without each decode person's Pj equipment :alculating Dj=u1zjmod p, and leaking the information concerning [that Dj is as a result of right count, and] zj The cipher verification approach characterized by proving to other decode persons, specifying the decode person Pj who failed in zero information certification as a deviation person, and other decode person equipments restoring a deviation person's secrecy value zj using secrecy value recovery procedure by zero information certification.
[Claim 14] It is the cipher verification approach characterized by for the secrecy restoration procedure to the exponent part to which each decode person equipment uses u1 as a bottom from the right (D1, --, Dn) in claim 12 or the cipher verification approach of 13 restoring D=u1z mod p, calculating m=e/Dmod p, and decoding Plaintext m.
[Claim 15] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order p of a multiplicative group Zp. Make g1 and g2 into the origin of Gp, make H into a general-purpose Hash Function, and it considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2modp, and Z=g1z mod p for an :ncryption procedure. (x1, x2, y1, y2, z) **Zq5 It contains. ** -- the cipher [as opposed to / carry out and / Plaintext m] E -- c -- as H(u1, u2) modp -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p -- three -- constructing (u1, u2, v) -- The processing which generates a random number r, the processing which receives Cipher E, and the processing which calculates c=H(u1, u2) mod q, The record medium which recorded :he program which makes the computer of decode person equipment perform processing which calculates V=(u1x1+cy1u2 x2+cy2v-1) r mod p, and processing which checks that it is V= 1 and verifies the justification of a cipher.
[Claim 16] V!=1 The processing which will exhibit BC (r) using a bit commitment function (BC) if it becomes, r which constitutes BC (r), x1 which constitutes public keys X and Y, x2, and y1 and y2 are used. (u1x1+cy1u2 x2+cy2v-1) The record medium characterized by including :he program which performs processing proved to a third party by zero information certification, without leaking the secrecy concerning [that the result of having performed count which becomes r mod p is V, and] r, x1, x2, and y1 and y2.
[Claim 17] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. Make g1 and g2 into the origin of Gq, make H into a general-purpose Hash Function, and n persons' decode person is set to P1-Pn. each decode person Pj -- the open value wj of a proper -- having -- **(x1, x2, y1, y2, z) Zq5 Distribute with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. The secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj is used as the decode person's Pj private key. Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p are used as the decode person's Pj public key. The processing which generates the secrecy value rj corresponding to the value wj which distributes random-number r**Zq with the secrecy variational method of threshold t, and is acquired, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p are used as a public key. It considers as the cipher of Plaintext m. A right cipher u1=g1r mod p, u2=g2r mod p, c=H (u1, u2), The processing which fills v=Xr Ycrmod p and e=mZr mod p, and receives cipher E= (u1, u2, v, e), The processing which calculates c=H (u1, u2), and the processing which calculates Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p, The processing which transmits the secrecy value Vjk corresponding to a value wk which distributes Vj with a verifiable secrecy variational method 2t or less more than threshold

, and is acquired to each decode person's Pk equipment, The processing which receives Vkj from all other decode person equipments Pk, and he processing which transmits Vj to all other decode person equipments, The processing which receives Vk from all other decode person :quipments, and the processing which transmits Vkj to all other decode person equipments, every -- with the processing which verifies that Vk s a right value using Vkj from all other decode person equipments Choose 2t+1 piece among the right and checked Vk, and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1. If equal and a restoration value is [a secrecy estoration procedure is similarly repeated in other 2t+1 piece combination and] all equal to 1 about no combination The record medium which ecorded the program which makes the computer of decode person equipment perform processing which judges that the cipher is inaccurate, ind will judge the cipher to be the right if there is combination set to 1 at least one.

[Claim 18] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. g1 and g2 are made into the origin of Gq, H is made into a general-purpose Hash Function, and it is **(x1, x2, y1, y2, z) Zq5. Private key, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) are used as a public key. the cipher E over Plaintext m -- c -- as H(u1, u2) mod q -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p - three -- constructing (u1, u2, v) -- it containing and with the processing which generates a random number r The processing which calculates x1'=x1 and rmod q, x2'=x2 and rmod q, y1'=y1 and rmod q, and y2'=y2 and rmod q using Above r, The processing which receives Cipher E, and the processing which calculates c=H(u1, u2) mod q, and calculates V=u1x1'+cy1' u2 x2'+cy2' v-rmod p from the received cipher, The record medium which recorded the program which makes the computer of decode person equipment perform processing which verifies the justification of a cipher when Above V checks that it is equal to 1.

[Claim 19] In the record medium of claim 18 when not equal to 1, V (X, Y, V) It receives that it is (x1, x2, y1, y2, r). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and V=u1x1r+cy1r satisfying u2 x2r+cy2 rv-rmod p -- zero information certification -- using (x1, x2, y1, y2, r), considering as secrecy The record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing proved to a verification person.

[Claim 20] dispersion of h to which g and h use g as a bottom in the record medium of claim 19 -- with the processing which is under Gq whose logarithm is strange and generates random numbers r, a1, a2, b1, and b2 R=gr ha mod p, RX1=Rx1ha1mod p, RX2=Rx2ha2mod p, RY1=Ry1hb1mod p and RY2=Ry2hb2mod p -- with the processing which exhibits R, RX1, RX2, RY1, and RY2 (X, Y, V, R, RX1, RX2, RY1, RY2) receive that it is (x1, x2, y1, y2, r, a, a1, a2, b1, b2). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, V=u1x1r+cy1r u2x2r+cy2r v-rmod p, R=gr ha mod p, RX1=Rx1ha1mod p, RX2=Rx2ha2mod p, RY1=Ry1hb1mod p, and RY2=Ry2hb2mod p -- the record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing which proves filling relational expression by zero information certification.

[Claim 21] In the record medium of claim 18, set n persons' decode person to P1-Pn, and w is used as the n-th root of 1 in mod q. Shall set wj to wj-1 mod q and wj!=1 shall be filled in 1<j<n. A value wj is assigned to each decode person Pj. The decode person's Pj private key (x2 j and y1 j, y2 x1j, j, zj) Distribute x1, x2, and (y1, y2, z) with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. Consider as the secrecy value corresponding to a value wj, and Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) are used as the decode person's Pj public key. Processing holding the secrecy value rj corresponding to a value wj which distributes random-number r**Zq with the secrecy variational method of threshold t, and is acquired, The processing which calculates and holds secrecy value x1j' corresponding to a value wj which distributes rx1, rx2, ry1, and ry2 with the secrecy variational method of threshold t, respectively, and is obtained, x2j', y1j', and y2j' by the distributed multiplication method, If a cipher is received, c=H (u1, u2) will be calculated and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p will be calculated. According to a broadcast mold channel The processing which transmits Vj to all other decode person equipments, and the processing which checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code, The record medium characterized by the above-mentioned program including the program which performs processing which verifies the justification of a cipher by checking that the value V restored with the secrecy restoration procedure to the above-mentioned exponent part is equal to 1 by above-mentioned computer.

[Claim 22] In the record medium of claim 21, 2 t<n shall be filled for threshold t. Instead of the processing which checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code Without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / right count, and] x1j', x2j', y1j', y2j', and rj The processing proved to other decode persons by zero information certification and the decode person Pj in whom zero information certification failed are specified as a deviation person. The record medium characterized by including the program which makes the above-mentioned computer perform a deviation person's secrecy value x1j', x2j', y1j', y2j', and processing that restores rj using secrecy value recovery procedure in the above-mentioned program.

[Claim 23] In the record medium of claim 21, when (V1, --, Vn) are not the codewords of a BCH code Without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj The processing proved to other decode persons by zero information certification and the decode person Pj who failed in the above-mentioned certification are specified with a deviation person. The record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing which restores a deviation person's secrecy value x1j', x2j', y1j', y2j', and rj using secrecy value recovery procedure.

[Claim 24] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. g1 and g2 are made into the origin of Gq, H is made into a general-purpose Hash Function, and it is **(x1, x2, y1, y2, z) Zq5. Private key, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) are used as a public key. It is verification equipment of the cipher to include. the cipher E over Plaintext m -- c -- as H(u1, u2) mod q -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p -- three -- constructing (u1, u2, v) -- A means to generate a random number r, and a means to calculate c=H(u1, u2) mod q, Cipher verification equipment characterized by having a means to calculate V=(u1x1+cy1u2 x2+cy2v-1) r mod p, and a means to verify the justification of a cipher when V checks that it is equal to 1.

[Claim 25] Cipher verification equipment characterized by having a means to prove that it is the result of V's using zero information certification when not equal to 1, and V calculating like r mod p (u1x1+cy1u2 x2+cy2v-1) to a random number r in the cipher verification equipment of claim 24 for a third party.

[Claim 26] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. Make g1 and g2 into the origin of Gq, make H into a general-purpose

Hash Function, and n persons' decode person is set to P1-Pn. each decode person Pj -- the open value wj of a proper -- having -- **(x1, x2, y1, y2, z) Zq5 Distribute with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. The secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj is used as the decode person's Pj private key. Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) are used as the decode person's Pj public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. The decode person Pj shall hold the secrecy value rj corresponding to a value wj which distributes random-number r**Zq with the secrecy variational method of threshold t, and is acquired. E= (u1, u2, v, e) is made into the cipher over the plaintext m which used 1x1g 2 x2modp of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p as the public key. A right cipher u1=g1r mod p, u2=g2r modp, c=H (u1, u2), A means to be verification equipment of the cipher with which are satisfied of v=Xr Ycrmod p and e=mZr mod p, and to calculate c=H (u1, u2) by receiving E, A means to calculate Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p, Vj is distributed with a verifiable secrecy variational method 2t or less more than threshold t. When Vkj is received from a means to acquire the secrecy value Vjk corresponding to a value wk, a means to transmit Vjk through a channel safe for each decode person's Pk equipment, and all other decode person equipments Pk, according to a broadcast mold channel If a means to transmit Vj to all other decode person equipments, and Vk are received A means to transmit corresponding Vkj to all other decode person equipments according to a broadcast mold channel, every -- with a means to verify using Vkj that Vk is a right value, and a means to choose 2t+1 piece among the right and checked Vk, and to restore V with the secrecy restoration procedure to exponent part A means to investigate whether the restored value V is equal to 1, and a means by which will repeat a secrecy restoration procedure similarly in other 2t+1 piece combination if it becomes, and V investigates [which is not equal to 1] whether V is equal to 1, Cipher verification equipment characterized by having a means to judge that the cipher is inaccurate if a restoration value is all equal to 1 about no 2t+1 piece combination, and to judge the cipher to be the right if there is combination set to 1 at least one.

[Claim 27] w is used as the n-th root of 1 in mod q in the cipher verification equipment of claim 26. Each decode person A means to set wj to wj-1 mod q, to consider as the characteristic value of disclosure of wj which fills wj!=1 in 1<j<n, and to calculate Dj=u1zjmod p, a means to transmit Dj to all other decode person equipments according to a broadcast mold channel, and the dispersion which uses as a bottom u1 which received (D1, --, Dn) -- the cipher verification equipment characterized by having a means to check that a logarithm is the codeword of a BCH code.

[Claim 28] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. g1 and g2 are made into the origin of Gq, H is made into a general-purpose Hash Function, and it is **(x1, x2, y1, y2, z) Zq5. Private key, 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) are used as a public key. It is verification equipment of the cipher to include. the cipher E over Plaintext m -- c -- as H(u1, u2) mod q -- u1=g1r mod p and u2=g2r mod p -- v=Xr Ycrmod p -- three -- constructing (u1, u2, v) -- A means to generate a random number r, and a means to calculate x1'=x1 and rmod q, x2'=x2 and rmod q, y1'=y1 and rmod q, and y2'=y2 and rmod q, A means to calculate c=H(u1, u2) mod q from the received cipher, Cipher verification equipment characterized by having a means to calculate V=u1x1'+cy1' u2 x2'+cy2' v-rmod p, and a means to verify the justification of a cipher when V checks that it is equal to 1 from this count result and a receiving cipher.

[Claim 29] In the cipher verification equipment of claim 28 V when not equal to 1 (X, Y, V) It receives that it is (x1, x2, y1, y2, r). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and V=u1x1r+cy1r u2x2r+cy2r satisfying v-rmod p -- zero information certification -- using (x1, x2, y1, y2, r), considering as secrecy Cipher verification equipment characterized by having a means to prove to verification person equipment.

[Claim 30] dispersion of h to which g and h use g as a bottom in the cipher verification equipment of claim 29 -- with a means to be under Gq whose logarithm is strange and to generate random numbers r, a1, a2, b1, and b2 R=gr ha mod p, RX1=Rx1ha1mod p, RX2=Rx2ha2mod p, RY1=Ry1hb1mod p and RY2=Ry2hb2mod p -- with a means to exhibit R, RX1, RX2, RY1, and RY2 (X, Y, V, R, RX1, RX2, RY1, RY2) receive that it is (x1, x2, y1, y2, r, a, a1, a2, b1, b2). 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, V=u1x1r+cy1r u2x2r+cy2r v-rmod p, R=gr ha mod p, RX1=Rx1ha1mod p, RX2=Rx2ha2mod p, RY1=Ry1hb1mod p, and RY2=Ry2hb2mod p -- the cipher verification equipment characterized by having a means to prove filling relational expression by zero information certification.

[Claim 31] n persons' decode person is set to P1-Pn in the cipher verification equipment of claim 28. Use w as the n-th root of 1 in mod q, and wj is set to wj-1 mod q. In 1<j<n, shall fill wj!=1 and a value wj is assigned to each decode person Pj. (x1, x2, y1, y2, z) **Zq5 Consider as a private key and 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p are used as a public key. The decode person's Pj private key (x2 j and y1 j, y2 x1j, j, zj) Distribute x1, x2, and (y1, y2, z) with the secrecy variational method of threshold t which fills 3 t<n, and are obtained. Consider as the secrecy value corresponding to a value wj, and Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1Zjmod p (Xj, Yj, Zj) are used as the decode person's Pj public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed, and it distributes random-number r**Zq with the secrecy variational method of threshold t. rx1, rx2, ry1, and ry2 are distributed with the secrecy variational method of threshold t with a means to acquire the secrecy value rj corresponding to a value wj, respectively. A means to calculate and obtain secrecy value x1j' corresponding to a value wj, x2j', y1j', and y2j' by the distributed multiplication method, About the received cipher, according to a means to calculate c=H (u1, u2), a means to calculate Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p, and a broadcast mold channel A means to transmit Vj to all other decode person equipments, and a means to check that the exponent part of (V1, --, Vn) is the codeword of a BCH code, Cipher verification equipment characterized by having a means to restore V with the secrecy restoration procedure to exponent part, and a means to verify the justification of a cipher by checking that the restored value V is equal to 1.

[Claim 32] In the cipher verification equipment of claim 31, 2 t<n shall be filled for threshold t. Instead of checking that the exponent part of (V1, --, Vn) is the codeword of a BCH code Without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / right count, and] x1j', x2j', y1j', y2j', and rj Cipher verification equipment characterized by having a means to prove to other decode persons by zero information certification.

[Claim 33] In the cipher verification equipment of claim 31, when (V1, --, Vn) are not the codewords of a BCH code Without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj Cipher verification equipment which specifies a means to prove to other decode persons by zero information certification, and the decode person Pj who failed in the certification with a deviation person, and is characterized by having a deviation person's secrecy value x1j', x2j', y1j', y2j', and a means to restore rj using secrecy value recovery procedure.

Translation done.]

DETAILED DESCRIPTION

Detailed Description of the Invention]
0001]
Field of the Invention] This invention relates to the cipher verification approach that a decode person verifies the justification of a cipher especially, and its program documentation medium, about the safe code approach that the information about a decode person's private key does not leak; also when the content of a communication link is kept secret when communicating by the electrical-communication system, and the content of decode is exhibited.
0002]
Description of the Prior Art] In a cryptosystem strong against a selection plaintext attack, a decode person verifies that the transmitting person of a cipher knows the original plaintext by a certain approach. A Cramer-Shoup code Paper R.Cramer and V.Shoup:"A practical public key cryptosystem provablysecure against adaptive chosen Were proposed by chipertext attack", Advances in Cryptology-CRYPTO'98 and LNCS 1462, Springer-Verlag, pp.13-25, and 1998. It is the public-key-encryption approach that it can prove that it is strong to an accommodative selection cipher attack under an assumption which is called existence of a general purpose one direction nature Hash Function and the difficulty of a Diffie-Hellman judging problem and which is believed widely. A Cramer-Shoup code is the code approach supposing one person's decode person with one private key corresponding to one public key.
0003] By the Cramer-Shoup code approach that it is already known in the case of the 1 decode person that it is strong to an accommodative selection cipher attack First, choose the big prime factors p and q so that q may divide p-1, and the origin g1 and g2 of the subgroup Gq of the order q of a multiplicative group Zp is used. It is **(x1, x2, y1, y2, z) Zq5 about a private key. A public key is set to 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p. The cipher E over plaintext m**Gq consists of (u1, u2, v, e), and the cipher created correctly satisfies u1=g1r mod p, u2=g2r mod p, c=H (u1, u2), v=Xr Ycrmod p, and e=mZr mod p to a certain random number r. First, c=H (u1, u2) is calculated and it verifies whether a cipher fills verification type u1x1+cy1u2 x2+cy2**v (mod p), the decode person who received this cipher refuses decode of that cipher, when not filling, when filling, calculates m=e/u1z modp and gets Plaintext m.
[0004] By the above-mentioned verification type, a decode person can check that the maker of a cipher knows the original plaintext m. Since decode is refused to the unjust cipher with which a verification type is not filled, as for an aggressor, information with useful any is not acquired, either. However, when refusing decode by this cipher verification approach as a result of verification, it is actually difficult to prove the information concerning [that the cipher verified to the third party does not serve as V!=v (mod p) as inaccurate / 2 (mod p) /, i.e., V**u1x1+cy1u2 x2+cy, and] V, without leaking information in any way.
[0005] Furthermore, by secrecy distribution distributing a corresponding private key to two or more partial private keys to one public key, and making this hold to two or more decode persons so that it may often be carried out by an ElGamal cryptosystem etc. As opposed to an unjust cipher with which a verification type is not filled in this code decode approach when the decode person of the manpower exceeding a threshold cooperates and it applies the decode with a threshold which enables it to decode a cipher Since the count result V of left part u1x1+cy1u2 x2+cy2 of a verification type becomes known to two or more decode persons, when the decode person who conspired with the aggressor exists, information is revealed to an aggressor and the safety to a selection cipher attack cannot be maintained.
[0006] the decode approach with a threshold -- paper V.Shoup and R.Gennaro: "Securing threshold cryptosystems against chosen ciphertext attack", Advances in Cryptology-EUROCRYPT, 98, LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 It is shown under an assumption called existence of random Oracle that the proposed method is strong to an accommodative selection cipher attack.
[0007] However, an assumption called random Oracle can obtain no guarantee about the safety, when it is very unreal and random Oracle is replaced and used for the Hash Function considered that the usual collision is difficult.
[0008]
[Problem(s) to be Solved by the Invention] In a Cramer-Shoup code, the object of this invention, without leaking the information about the value in a verification type entirely When the justification of a cipher can be verified and it is shown that the value of a verification type is not just When the decode person of further plurality [prove / for a third party] cooperates and verifies that the value is created correctly by zero information certification, even if there is an inaccurate person in a decode person The value of a verification type is to offer the cipher verification approach which is not revealed to a decode person, either, its program documentation medium, and its equipment.
[0009]
[Means for Solving the Problem] The exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code is carried out with the random number with which everyone of a decode person cannot know the value, and the justification of a cipher is verified by verifying whether the result of having carried out the exponentiation is set to 1. Count of carrying out a exponentiation by these random numbers, by carrying out by cooperation of a total-session person by distributed count Also when not filling a verification type, the value of the verification type before carrying out a exponentiation is revealed to no decode person, and it is got blocked. When not just Since calculated value turns into a value which is not 1 and the exponentiation of the value is carried out by the random numbers, even if the value by which the exponentiation is carried out is shown and it is shown that calculated value is not 1, i.e., are not just, the value in front of the exponentiation is hidden, and there is no possibility that information may leak.

0010] Setting n persons' decode person to P1-Pn, each decode person Pj (j= 1, 2, --, n) shall have the open value wj of a proper. (x1, x2, y1, 2, z) **Zq5 It distributes with the secrecy variational method of threshold t, and let the secrecy value (x2 j and y1 j, y2 x1j, j, zj) orresponding to a value wj be the decode person's Pj private key.
0011] Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. It onsiders as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) for encryption. It shall onnect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it s guaranteed to be to receive a content with other all the members' same decode person equipment.
0012] E= (u1, u2, v, e) is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment erforms a distributed random-number generation procedure in cooperation, and the decode person's Pj equipment acquires the secrecy value j. Here, rj is a secrecy value corresponding to the value wj at the time of distributing random-number r**Zq with the secrecy variational nethod of threshold t, and is the value which can recover r with a secrecy decode procedure from the secrecy value of t+1 piece of arbitration. Moreover, each decode person equipment cannot know the value of r, but r becomes the random integer of under or more 0q from the property f a distributed random-number generation procedure.
0013] The equipment of each decode person Pj who received E calculates c=H (u1, u2) and Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p. urthermore, Vj is distributed with a with a threshold [of 2t] verifiable secrecy variational method, and the secrecy value Vjk corresponding to value wk (k= 1, 2, --, n, k!=j) is transmitted through a channel safe for each decode person's Pk equipment. After receiving Vjk from all other lecode person equipments, the decode person's Pk equipment transmits Vk to all other decode person equipments through a broadcast mold hannel. As for each decode person equipment, each Vk which received verifies using Vkj that it is a right value.
0014] 2t+1 piece is chosen among the right and checked Vk, and it investigates whether the value V restored with the secrecy restoration rocedure to exponent part, i.e., x1k+cy1k, and x2k+cy2k is equal to 1. If not equal, a secrecy restoration procedure will be similarly repeated n other combination, and if a restoration value is all equal to 1 about no 2t+1 piece combination, decode will be refused and it will stop.
0015] the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned rocedure] the exponent part from the right Vk of the arbitration beyond 2t+1 piece -- V=(u1x1+cy1u2 x2+cy2v-1) r mod p -- V can be estored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of erification type u1x1+cy1u2 x2+cy2 in law] v. On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an riginal verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed andom-number generation procedure to be set to 0 are 1/q, and since they are small enough, they can be disregarded. Therefore, V can onsider in cooperation with [an original verification type] v, when in cooperation with 1.
0016] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value / of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the bject of ** of making it the value V of the verification type to the just cipher E not set to 1 [or] First, in order to make the object of (1) uccessful, it must be made for the value of V restored from a certain 2t+1 piece Vk to be set to 1. However, before all decode person quipments including inaccurate person equipment get to know the value of Vk which other decode person equipments take out Since the value f Vk of self-equipment cannot be changed after having to distribute the value of one's Vk by the verifiable secrecy distribution approach and etting to know the value of Vk of other decode person equipments Only when the anticipation about Vk of other decode person equipments omes true, an inaccurate decode person can attain the object of (1). The probabilities for anticipation to come true are 1/q, and since they are mall enough, they can be disregarded. Next, since an inaccurate person is at most t persons and, as for other 2t+1 person equipments, the right value is transmitted even if inaccurate decode person equipment transmits what kind of unjust value Vk about the case of (2), the whole of at east one kind can take the set which consists of 2t+1 piece Vk of a right value, and V= 1 is restored from such a set.
0017] Since one value of r which fills V=(u1x1+cy1u2 x2+cy2v-1) r mod p to any values of u1x1+cy1u2 x2+cy2 about informational leakage when V is not 1 becomes settled Even if the value of (u1x1+cy1u2 x2+cy2v-1) is randomized by r and shows this randomized value, the value before being randomized by r does not leak, that is, the information about u1x1+cy1u2 x2+cy2 does not leak at all by the above-mentioned verification approach.
0018] As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according to this invention is less than [of all decode persons] 1/3, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's ode decode equipment strong against an accommodative selection cipher attack can be constituted.
0019] When n decode persons are in the above technique, to n data for verification (V1, --, Vn) received from all decode person equipments, ach decode person equipment takes out 2t+1 piece data, and verifies whether a certain verification type is satisfied. When not satisfied, this erification is performed to all the 2t+1 piece combination that can be taken to n pieces. Therefore, in not satisfying a verification type, it has he fault that computational complexity increases exponentially, to several n of a decode person.
0020] According to another viewpoint of this invention, in the code decode approach by two or more decode persons, the cipher verification pproach and its program documentation medium of a code strong against the accommodative selection cipher attack which can be recovered even if it can perform count efficiently also to many decode persons and 1/3 or more decode persons perform injustice are offered. That is, as a neans to reduce the computational complexity to the number of decode persons, by making each decode person equipment prove the ustification of that result by zero information certification, an inaccurate person is specified and, according to another viewpoint of this nvention, a cipher is first verified only using just data. By doing so, it is possible to verify by the computational complexity proportional to everal n of a decode person. However, since there is much traffic, when injustice hardly happens, effectiveness is bad [the zero information ertification used in this case]. When a right cipher is received by setting the open value of each decode person's proper that the count result of ach decode person equipment serves as a codeword of a BCH code, and addressee equipment verifying that a count result is a codeword, and performing zero information certification only when it is not a codeword, it becomes possible to perform efficient count, with traffic stopped.
0021] If based on this approach, the number of the inaccurate persons who can approve is to t persons who fill 3t+1>n, and when a safe system with more high tolerance is desired, it is unsuitable. Moreover, although it also becomes bored when an inaccurate person is less than [1/3 or more] 1/2, and other decode person equipments compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified as a means, a technical problem is solved by enabling it to calculate a right

esult instead of the inaccurate decode person.
0022] The concrete means is as follows. n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode erson Pj. Threshold t which fills 3 t<n is defined. (x1, x2, y1, y2, z) **Zq5 It distributes with the secrecy variational method of threshold t, nd let the secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj be the decode person's Pj private key.
0023] Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. It onsiders as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) for encryption. It shall onnect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it s guaranteed to be to receive a content with other all the members' same decode person equipment.
0024] E= (u1, u2, v, e) is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment erforms a distributed random-number generation procedure in cooperation, and the decode person's Pj equipment acquires the secrecy value j. Here, rj is a secrecy value corresponding to the value wj at the time of distributing random-number r**Zq with the secrecy variational nethod of threshold t, and is the value which can recover r with a secrecy decode procedure from the secrecy value of t+1 piece of arbitration. Moreover, each decode person cannot know the value of r, but r becomes the random integer of under or more 0q from the property of a listributed random-number generation procedure.
0025] Next, all decode person equipments cooperate, and perform a distributed multiplication means, and each decode person's Pj equipment btains secrecy value x1j', x2j', y1j', and y2j'. Secrecy value x1j' is a value which distributes the product of a random number r and a private ey x1 with the secrecy variational method of threshold t, and is acquired, and can decode x1j' to r-x1 (mod q) which t+1 person's decode erson of arbitration has here. r and x2 (mod q), r-y1 (mod q), and r-y2 (mod q) can be similarly restored from the value of t+1 piece of rbitration about secrecy value x2j', y1j', and y2j', respectively.
0026] Each decode person Pj equipment which received E calculates c=H (u1, u2) and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p, and transmits Vj to all other decode person equipments through a broadcast mold channel. Next, each decode person equipment checks that the exponent part f (V1, --, Vn) is the codeword of a BCH code. When it becomes clear not the codeword of a BCH code but that it is not right, the exponent art of (V1, --, Vn) each decode person's Pj equipment It proves to other decode persons by zero information certification, without leaking the nformation concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj.
0027] It considers that the decode person Pj who failed in certification is an inaccurate person, and other decode person equipments recover ecrecy value x1j' of the deviation person who is the inaccurate person, x2j', y1j', y2j', and rj using secrecy value recovery procedure, and he exhibits the value of the right Vj. The rights (V1, --, Vn) including the value of the exhibited right Vj are obtained. After the exponent part of V1, --, Vn) checks the right thing and that it is a codeword, the secrecy restoration procedure to exponent part restores a value V. Each decode erson equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop.
 [0028] If equal, each decode person's Pj equipment will calculate Dj=u1zjmod p, and will transmit it to all other decode person equipments according to a broadcast nold channel. Each decode person equipment which received Dj verifies the codeword same with having carried out to (V1, --, Vn) to (D1, --, Dn), when injustice is detected, performs zero information certification similarly, specifies an inaccurate person, and it recovers the value of the right Dj using secrecy value recovery procedure.
0029] From the right (D1, --, Dn), with the secrecy restoration procedure to exponent part, each decode person equipment restores D=u1z mod p, calculates m=e/Dmod p, and decodes Message m. the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right Vk of the arbitration beyond 2t+1 piece -- V= (u1x1+cy1u2 x2+cy2v-1) r mod p -- V can be restored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type u1x1+cy1u2 x2+cy2 in law] v. On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are 1/q, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v, when in cooperation with 1.
[0030] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the bject of ** of making it the value V of the verification type to the just cipher E not set to 1 [or] However, the output of all decode person equipments can detect the existence, if an unjust value is less than [of the whole] 1/3 when an unjust value exists since it is verified by codeword inspection of a BCH code. In such a case, since each decode person proves the rightness of an output value by zero information certification, the inaccurate person who outputted the unjust value fails in certification, and is eliminated.
0031] About informational leakage, when V is not 1, since one value of r which fills V=(u1x1+cy1u2 x2+cy2v-1) r mod p to any values of u1x1+cy1u2 x2+cy2 becomes settled, by the above-mentioned verification approach, the information about u1x1+cy1u2 x2+cy2 does not leak it all. As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according to this invention is less than [of all decode persons] 1/3, by cooperation of two or more decode person, it is possible to calculate a verification ype equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode approach strong against an accommodative selection cipher attack can be constituted.
0032] By computing and exhibiting the distributed private key which codeword inspection of a BCH code is not conducted, but zero information certification is always performed in the above-mentioned means on the other hand, an inaccurate person is specified, other decode persons cooperate, and the inaccurate decode person has Although it also becomes bored, since a right result is calculable instead of the inaccurate decode person, it can respond to less than 1/2 inaccurate person (in order to determine by majority that zero information certification is right, one half of decode persons at least must be right).
0033]
[Embodiment of the Invention] The cipher verification approach which is the first example of this invention is explained to one or less example. The cipher created with cipher implementer equipment 11 as shown in drawing 1 is decoded with decode person equipment 12. If it is not a right cipher, in order to avoid carrying out decode refusal freely with decode person equipment 12, it verifies whether decode refusal is appropriate with verification person equipment 13.
[0034] There shall be the big prime factors p and q now, and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. It considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p for an encryption procedure. Here, it is **(x1,

:2, y1, y2, z) Zq5. It carries out. The public key shall be exhibited with p, q, g1, and g2 as a open parameter. Moreover, the private key shall be :tored on the memory of decode person equipment.
0035] As shown in drawing 2 , after receiving cipher E= (u1, u2, v, e) of the plaintext m enciphered by the Cramer-Shoup code approach vhich used X, Y, and Z as the public key (S1), Decode person equipment generates a random number r (S2), and calculates c=H (u1, u2) and V=(u1x1+cy1u2 x2+cy2v-1) r mod p (S3). If V becomes one, this cipher will be considered as acceptance and (S4) and decode count will be performed (S5).
0036] If V is not 1, it will consider as a rejection. In order to prove that it is a rejection to a third party, BC (r) is exhibited using bit commitment function BC(). There are some which are depended on Pedersen in this bit commitment function. That is, a random number s is generated and it calculates with BC(r, s):=gr hs mod p. dispersion of h to which g and h use g as a bottom here -- it is under Gq whose logarithm is strange.
0037] r which constitutes BC (r, s), x1 which constitutes public keys X and Y, x2, and y1 and y2 -- using -- r mod p (u1x1+cy1u2 x2+cy2v-1) -- it proves to a third party by zero information certification, without leaking the secrecy concerning [that the result of having calculated is V, and] r, x1, x2, and y1 and y2 (S6). [then,] The following procedures perform this zero information certification.
0038] dispersion of h which uses g as a bottom for g and h below -- it considers as the origin of Gq whose logarithm is strange. decode person equipment -- random numbers a, a1, a2, b1, and b2 -- Zq -- choosing -- R=gr ha mod pRX1=Rx1ha1 modpRX2=Rx2ha2 modpRY1=Ry1hb1 modpRY2=Ry2hb2 modp -- R, RX1, RX2, RY1, and RY2 are sent to verification person equipment.
0039] Furthermore, decode person equipment chooses a random number w0 from Zq as random, and is K=g and L=gw0. mod p is sent to verification person equipment. Verification person equipment calculates B=Ke0Le1 modp by choosing e0 and e1 from Zq as random, and sends B to decode person equipment.
0040] Decode person equipment chooses random numbers w1-w18 from Zq as random. T1 =g1 w1g2 w2 mod pT2 =g1 w3g2 w4 mod pT3 =gw5gw6 mod pT4 = Rw1hw7 mod pT5 =Rw2hw8 mod pT6 =Rw3hw9 mod pT7 =Rw4hw10 mod pT8 = Calculate gw11 hw12 mod pT9 =gw13 hw14 mod pT10=gw15 hw16 mod pT11=gw17 hw18 mod pT12=u1w11+cw15u2w13+cw17 v-w5 mod p. It sends to verification person equipment.
0041] Verification person equipment sends e0 and e1 to decode person equipment.
Decode person equipment checks that B=Ke0Le1 modp is realized, and when not realized, it stops certification. When this is realized, Decode person equipment is z1=w1+e0 and x1 modqz2=w2+e0 and x2 modqz3=w3+e0 and y1 modqz4=w4+e0 and y2 modqz5=w5+e0 and r. modqz6=w6+e0anda modqz7=w7+e0 and a1 modqz8=w8+e0 and a2 modqz9=w9+e0 and b1 modqz10=w10+e0 and b2 modqz11=w11+e0 and r-x1 modqz12=w12+e0 (a-x1+a1) modqz13=w13+e0, r, and x2 modqz14=w14+e0 (a and x2+a2) modqz15=w15+e0 and r-y1 modqz16=w16+e0 (a-y1+b1) modqz17=w17+e0 and r-y2 modqz18=w18+e0 (a-y2+b2) modq It calculates and z1-z18, and w0 are sent to verification person equipment.
0042] Verification person equipment L=gw0 modpg1 z1g2 z2=T1 Xe0mod pg1 z3g2 z4=T2 Ye0mod pgz5hz6=T3 Re0 modpRz1hz7=T-four e(RX1)0mod pRz2hz8=T5 e(RX2)0mod pRz3hz9=T6 e(RY1)0mod pRz4hz10 =T7 e(RY2)0mod pgz11 hz12 =T8 e(RX1)0mod pgz13 hz14 =T9 e(RX2)0mod It verifies that pgz15 hz16 =T10(RY1) e0mod pgz17 hz18=T11(RY2) e0mod plutonium1z11+cz15u2z13+cz17 v-z5 =T12Ve0mod p is realized.
0043] The principle of the upper certification is Schnorr. It is the same as that of a signature, and since a verification type is realized only when decode person equipment creates correctly V, X, Y, R, RX1, RX2, RY1, and RY2, when at least one is not realized, verification is considered as failure.
The second example of this invention is explained to two or less example. As shown in drawing 3 R> 3, they are code implementer equipment 11 and 121-12n of each equipment of the decode persons P1-Pn. It connects with the broadcast mold channel 14, and is 121-12n of decode person equipment. It connects by the channel 15 safe for mutual.
0044] There shall be the big prime factors p and q now, and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. First, n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode person Pj (j= 1, 2, --, n). Threshold t which fills 3 t<n is defined. All decode person equipments perform the distributed random-number generation procedure of threshold t 3 times, and the decode person's Pj equipment acquires a secrecy value (x2 j and y1 j, y2 x1j, j, zj), and makes this the decode person's Pj private key. Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. Furthermore, it considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p for an encryption procedure. Here, it is **(x1, x2, y1, y2, z) Zq5. It is the random number restored by the secrecy restoration procedure from t+1 set of secrecy values (x2 j and y1 j, y2 x1j, j, zj) of arbitration. There is an approach by Pedersen in the distributed random-number generation procedure which generates such a random number. Below, the distributed random-number generation procedure is shown.
0045] Between each decode person equipment, as shown in drawing 3 , there shall be a safe channel 15 and each decode person equipment shall use the broadcast mold channel 14 it is guaranteed to be to receive a content with other all the members' same decode person equipment.
S-1) the equipment of Pj -- two polynomials on Zq -- f(X) =a0 j+a1jX+--+atjXt And gj (X) =b0 j+b1jX+--+btjXt random -- choosing -- every -- fj (wk) and gj (wk) are transmitted to the equipment except for 1, 2, --, n, and k=j k= -- of Pk through a safe channel.
0046] S-2) The equipment of Pj calculates Cij=g1aij g2bij mod p to i= 1, --, t, and transmits it to all other decode person equipments through a broadcast mold channel.
S-3) The equipment of Pk which received Cij from all other decode person equipments is g1fj(wk) g2gj(wk) =C0jwk0 and C1jwk1 as wki=wki mod q. -- It verifies that Ctjwkt mod p is realized.
0047] S-4) The equipment of Pk is x1 k=f1(wk)+f2(wk)+. -- They are +fn(wk) mod q and x2k=g1(wk)+g2(wk)+. -- Distributed random-number value x1k and x2k are obtained as +gn(wk) mod q.
S-5) X=C00, C01 -- It is referred to as C0n modp. Private key y1j, y2j, and zj to which public keys Y and Z and each decode person correspond similarly are also created similarly.
0048] All decode person equipments generate distributed random-number r**Zq with a distributed random-number generation procedure, and each decode person's Pj equipment holds the secrecy value rj (drawing 5 , S1). After receiving cipher E= (u1, u2, v, e) of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y, and Z as the public key (S2), each decode person's Pj equipment calculates c=H (u1, u2) and Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p (S3).

0049] Then, the equipment of Pj distributes Vj with a with a threshold [of 2t] verifiable secrecy variational method, and the secrecy value Vjk corresponding to a value wk is transmitted through a channel safe for each decode person's Pk equipment (S4). The approach of Pedersen can be used for the verifiable secrecy variational method used here. The following is the procedure.
P-1) g and h which there are the big prime factors P and Q, and Q divides P-1, and are made into Q>p are GQ whose value of log g h is strange. It considers as origin.
0050] P-2) the equipment of Pj -- ZQ Two upper polynomials fj (X) =Vj+a1jX+--+atjXt And gj (X) =b0 j+b1jX+--+btjXt (however, it considers as a0 j=Vj) -- the part of Vj -- removing -- random -- choosing -- every -- fj (wk) and gj (wk), i.e., Vjk, are transmitted to the equipment of Pk through a safe channel.
P-3) The equipment of Pj calculates Cij=gaij hbij mod p to i= 1, --, t, and transmits it to all other decode person equipments through a broadcast mold channel.
0051] P-4) The equipment of Pk which received Cij is gfj(wk) hgj(wk) =C0jwk0 and C1jwk1 as wki=wki mod q. -- It verifies that Ctjwkt mod p is realized, that is, Vjk is verified (S5).
P-5) When not realized, the equipment of Pk transmits a "rejection" to all other decode person equipments through a broadcast mold channel.
0052] When advice of P-6 "a rejection" is t+1 or more pieces, it is considered that Pj is an inaccurate person, it is eliminated (S6), and all other decode person equipments discard all the information that the equipment of Pj transmitted before. The step of P-4, and 5 and 6 is the procedure of performing verification of the distributed secrecy value Vjk, and an inaccurate person's abatement, and after all decode person equipments finish transmitting data, you may carry out by releasing a rejection list collectively.
[0053] After all decode person equipments distribute Vj with the above-mentioned procedure, each decode person's Pj equipment transmits Vj and b0j to all other decode person equipments through a broadcast mold channel (S7). The equipment of each decode person Pj who received this checks that C0 j=g1Vjhb0j mod p is realized, and verifies Vj (S8). When not realized, like the above, a "rejection" is notified to all other decode person equipments, and an inaccurate person is eliminated (S9).
[0054] 2t+1 piece is chosen as arbitration from the right and all checked Vk(s) (S10), and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1 (S11). The secrecy restoration procedure to exponent part is reference. Cramer, et.al: "A seure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed. The restoration procedure to the exponent part at the time of setting to alpha the set of the index k of 2t+1 piece Vk chosen as below is shown. The secrecy value of exponent part presupposes that it is the secrecy value acquired with the verifiable secrecy variational method of Pedersen.
[0055] R-1) It is a Lagrange interpolation multiplier first [0056]
[Equation 1]
$$\lambda_{j,\alpha} = \Pi_{k \in \alpha,\ k \neq j}\ j/(j-k)$$

It calculates by carrying out.
R-2) Next, [0057]
[Equation 2]
$$V = \Pi_{j \in \alpha}\ V_j^{\lambda j,\alpha} \mod p$$

It calculates. If V is not 1, a secrecy restoration procedure will be similarly repeated in other 2t+1 piece combination (S12). If a restoration value is all equal to 1 about no combination, a rejection will be notified and it will stop.
[0058] If there is combination set to 1 at least one, this cipher will be considered as acceptance. Each decode person's Pj equipment calculates Dj=u1zjmod p, as shown in drawing 4 R> 4 (S1), and it transmits it to all other decode person equipments according to a broadcast mold channel (S2). the dispersion to which each decode person equipment which received Dj uses u1 of D1, --, Dn as a bottom -- by checking that a logarithm is the codeword of a BCH code, if it is (S4) and a codeword, the secrecy restoration procedure to the above-mentioned exponent part will restore D=u1z mod p (S5), m=e/D modp will be calculated, and Message m will be decoded (S6). If it is not a codeword in step S4, what is made to prove the rightness of count and cannot be proved by zero information certification will be discarded as inaccurate Di (S7).
The third example of this invention is explained to three or less example.
[0059] A safe channel shall be between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment. There shall be the big prime factors p and q and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. First, n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode person Pj. Threshold t which fills 3 t<n is defined.
[0060] First, the secrecy distribution approach by Pedersen is shown. First, g and h It considers as the origin of Gq whose logg h is strange. The equipment of the portioner P who distributes the secrecy values a0 and b0 is t-th two polynomials f(X) =a0+a1X+ on Zq. -- It is +atXt and g(X) =b0+b1X+. -- It is +btXt. Except for a0, it chooses at random, and f (wj) and g (wj) are sent to each addressee's Pj equipment through a safe channel.
[0061] Next, the commitment value Ei of each multiplier is calculated like Ei=gaihbimod p to i= 0, --, t, and it opens to the public through a broadcast mold channel. Each equipment of Pj which received these is gf (wj) as uji=wji mod q. hg (wj) =E0uj0 E1uj1 -- It verifies that Etujt mod p is realized. This E0uj0 E1uj1 -- The value of Etujt mod p is called the commitment to the distributed secrecy value of Pj. If the commitment value of each multiplier is exhibited, anyone can also calculate the commitment to which distributed secrecy value of Pj.
[0062] Below, it is Ped (a0, b0) about this secrecy distribution approach [g, h]. -> (a0j, b0j) (E0, --, Et)
** -- it writes like. (a0, b0) are confidential information distributed, each equipment of Pj is the distributed secrecy value received through a safe channel, and its (a0j, b0j) are equal to f (wj) and g (wj) respectively. (E0, --, Et) are commitment values of each multiplier exhibited through a broadcast mold channel. [g, h] express the bottom used in case a commitment is created. As long as there is especially no notice about the above-mentioned notation, the multiplier of the polynomial except a constant term shall be chosen at random.
[0063] Thus, from the distributed secrecy value, when polynomial interpolation recovers the original secrecy, the holder of each distributed secrecy value exhibits the value first. It is ga0j hb0j =E0uj0 E1uj1 to the exhibited value (a0j, b0j). -- It checks that Etujt modp is realized. The set which that index j makes is set to alpha about t+1 (a0j, b0j) of arbitration of which this formula consists. It is a Lagrange interpolation

nultiplier [0064]
Equation 3]
$\lambda_{i,\alpha} = \Pi_{k\in\alpha,\ k\neq i} j/(j-k) \bmod q$

t is [0065] when it carries out.
Equation 4]
$\Sigma_{j\in\alpha} \lambda_{i,\alpha}\ a0j \bmod q = a0$

\ next door and a0 are recoverable. b0 is recoverable similarly. The above-mentioned secrecy distribution approach can completely be similarly performed, even if it uses only one bottom. In such a case, it is written as Ped(a0) [g] -> (a0j) (E0, --, Et).
0066] The random number distributed in cooperation by two or more persons is generable using this secrecy distribution approach. First, the equipment of Pi chooses random numbers ai and bi from Zq, and is this Ped(ai, bi) [g, h] -> (aij, bij) (Ei0, --, Eit)
** -- it distributes like. All the members of P1-Pn perform this. Then, the equipment of Pj receives (a1j, b1j), --, (anj, bnj) from a safe channel, and receives (E10, --, E1t), --, (En0, --, Ent) from a broadcast mold channel. At this time, it is the distributed secrecy value (x1j, x2j) of Pj x1j=a1j+ -- +anj modq, x2j=b1j+ -- It is referred to as +bnj modq. The random-number value x1 recovered from this distributed secrecy value is [0067].
Equation 5]
$x1 = \Sigma_{j\in\alpha} \lambda_{k,\alpha}\ x1\ j = a1 + \cdots + an \bmod q$

The value is known by nobody until it comes out, and it is and recovery is performed. Moreover, the commitment value EXk of the k-th multiplier of the polynomial which makes this secrecy random-number value a constant serves as EXk=E1 k-E2 k--Enkmod p. Especially, it is cautious of it being EX0=gx1hx2mod p. This approach is called distributed random-number generation, and it is Rand([a], [b]) [g, h] -> (aj, bj) (E0, --, Et).
It writes. ([a] [b]) is a random-number value generated and means that the value of [ ] is strange to every calculator. [g, h] -- and [of semantics] (aj, bj) (E0, --, Et) is the same as that of the notation of the above-mentioned secrecy distribution.
[0068] All decode person equipments are the distributed random-number generation procedure of threshold t Rand([x1], [x2]) [g1, g2] -> (x1j, x2j) (EX0, --, EXt)
Rand([y1], [y2]) [g1, g2] -> (y1j, y2j) (EY0, --, EYt)
Rand ([z1]) [g1] -> (z1j) (EZ0, --, EZt)
** -- performing 3 times like, the decode person Pj acquires a secrecy value (x2 j and y1 j, y2 x1j, j, zj), and makes this the decode person's Pj private key. Moreover, let Xj=g1x1j g2 x2jmod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. Furthermore, it considers as the public key which uses X=EX0=g1x1g2 x2modp, Y=EY0=g1y1g2y2mod p, and Z=EZ0=g1z mod p for an encryption procedure. It is **(x1, x2, y1, y2, z) Zq5 here. It is the random number restored by the secrecy restoration procedure from t+1 set of secrecy values (x2 j and y1 j, y2 x1j, j, zj) of arbitration.
[0069] All decode person equipments perform distributed random-number generation procedure Rand ([r], [s]) [g1, g2] -> (rj, sj) (R0, --, Rt), and generate distributed random-number r**Zq, and each decode person's Pj equipment holds the secrecy values rj and sj (drawing 6 , S1). R is set to R=R0=g1r g2second mod p here.
[0070] Next, all decode person equipments obtain secrecy value x1j', x2j', y1j', and y2j' with a distributed multiplication means (S2). Secrecy value x1j' is a value which distributes the product of a random number r and a private key x1 with the secrecy variational method of threshold t, and is acquired, and can decode rx1 (mod q) here from x1j' which t+1 person's decode person of arbitration has. rx2 (mod q), ry1 (mod q), and ry2 (mod q) can be similarly restored from the value of t+1 piece of arbitration about secrecy value x2j', y1j', and y2j', respectively. About such a distributed multiplication means, it performs as follows.
[0071] The decode person's Pj equipment is Ped(x1j, x2j) [g1, g2] -> (x1ji, x2 ji) (EXj0, --, EXjt).
It performs. Each equipment of Pj calculates Rj=g1rjg2sjmod p. This value Rj is Rj=R0uj0 R1uj1 as uji=wji mod q. -- Since you may calculate like Rtujt mod p, it is cautious of the ability of anyone to calculate.
[0072] Next, the polynomial used for distributing x1j and x2j by Ped (x1j, x2j) is used for the equipment of Pj as it is, and it is Ped(x1j, s1j) [Rj, g2] -> (x1ji, s1ji) (ERX 1j0, --, ERX1jt).
Ped(x2j, s2j) [Rj, g2] -> (x1ji, s2ji) (ERX 2j0, --, ERX2jt)
It performs. However, s1j and s2j also choose at random the polynomial which chooses at random and makes these a constant term.
[0073] To the last, the equipment of Pj is Ped(x1 j-rj, x1j-sj+s1j) [g1, g2] -> (rx1ji, rs1ji) (ERX 1j0, --, ERX1jt).
Ped(x2j-rj, x2j-sj+s2j) [g1, g2] -> (rx2ji, rs2ji) (ERX 2j0, --, ERX2jt)
It carries out.
[0074] Each equipment of P1-Pn performs the above-mentioned procedure. The equipment of Pi is the set (rx11i, --, rx1ni) of a distributed secrecy value which received to a Lagrange interpolation multiplier [0075]
[Equation 6]
$\lambda_{j,\alpha} = \Pi_{k\in\alpha,\ k\neq j} j/(j-k)$ として、

$$x1\ j' = \Sigma_{j\in\alpha} \lambda_{j,\alpha}\ r x1\ j\ i \bmod q$$

It calculates. The set of the index of right x1j' is set to beta, and it is [0076] at the time of |beta|>=t+1.
[Equation 7]

$$\Sigma_{j\in\beta}\lambda_{j,\beta}\ x1\ j' = \Sigma_{j\in\beta}\{\lambda_{j,\beta}\ \Sigma_{j\in\alpha}\lambda_{i,\alpha}\ r\ x1\ i\ j\}$$

$$= \Sigma_{i\in\alpha}\lambda_{i,\alpha}\ \{\Sigma_{j\in\beta}\lambda_{j,\beta}\ r\ x1\ i\ j\}$$

$$= \Sigma_{i\in\alpha}\lambda_{i,\alpha}\ r\ i\cdot x1\ i = r\cdot x1$$

since a next door and multiplication result r-x1 are recoverable, it turns out that x1j' is the t-th distributed secrecy value of r-x1. x2j' as well as :1j' is calculated. Furthermore, a distributed multiplication procedure is similarly performed and calculated about secrecy value y1j' and y2j'.
0077] After receiving cipher E= (u1, u2, v, e) to the plaintext m enciphered by the Cramer-Shoup code approach (S3), each decode person's Pj :quipment c=H (u1, u2) and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p are calculated, and Vj is transmitted to all other decode person equipments hrough (S4) and a broadcast mold channel (S5). Next, as for each decode person equipment, the exponent part of (V1, --, Vn) checks that it is he codeword of a BCH code (S6). A codeword verification procedure reference F.J.MacWilliams : "The Thory of Error Correcting Codes", Jorth-Holland Mathematical Library, and pp.201-202 -- or M. Ben-Or and S.Goldwasser, A. Wigerson:" Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation" and 20 th ACM Symposium on Theory It is detailed to of Computing, pp.1-10, and :988. A codeword verification procedure is shown below.
w!=1 is used as the n-th root of 1 in mod q, and it is referred to as xiij=wj (i-1) modq.
It is [0078] about j= 1, --, all 2t j.
Equation 8]

$$V1^{\xi 1j}\ V2^{\xi 2j}\cdots Vn^{\xi nj}\ \mathrm{mod}\ p = 1$$

t checks becoming. When it becomes clear with the above-mentioned procedure that the exponent part of (V1, --, Vn) is not right, each decode person's Pj equipment It proves to other decode person equipments by zero information certification, without leaking the information :oncerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj (S7).
0079] This zero information certification is performed as follows. However, by explanation of the procedure to following Pj, since Subscript j s attached to all variables, this is excluded and explained. First, distributed secrecy value x1' which Pj holds, x2', y1', y2', and r are received. a, 11, a2, and b1 as a certain random number R=g1r g2second mod pRX1=ERX10=Rx1g2a1mod pRX2=ERX20=Rx2g2a2mod pRY1=ERY10=Ry1g2b1mod pRY2=ERY20=Ry2g2b2mod The values R, RX1, RX2, RY1, and RY2 of a commitment p Becoming can be acquired from the commitment value of the multiplier exhibited with the distributed random-number generation means and the distributed multiplication means to anyone.
0080] Pj chooses a random number w0 from Zq as random, and sends K=g and L=gw0mod p to other decode person equipments. Other decode person equipments cooperate and are Rand([e0], [e1]) [K, L] -> (e0i, e1i) (Ee0, --, Eet).
It performs and Ee0=Ke0Le1mod p is sent to the equipment of Pj.
[0081] The equipment of Pj chooses random numbers w1-w18 from Zq as random. T1 =g1w1g2 w2 modpT2 = g1 w3g2 w4 modpT3 =gw5gw6 modpT4 =Rw1hw7 modpT5 = Rw2hw8 modpT6 =Rw3hw9 modpT7 =Rw4hw10modpT8 = Calculate gw11 hw12 mod pT9 =gw13 hw14 mod pT10=gw15 hw16 mod pT11=gw17 hw18 mod pT12=u1w11+cw15u2w13+cw17 v-w5 modp. It sends to other decode person equipments.
[0082] Other decode person equipments exhibit a distributed secrecy value, recover e0 and e1, and send them to the equipment of Pj. The equipment of Pj checks that Ee0=Ke0Le1 modp is realized, and when not realized, it stops certification. When this is realized, The equipment of Pj S1=w1+e0 and x1mod qS2=w2+e0andx2mod qS3=w3+e0andy1mod qS4=w4+e0andy2mod qS5=w5+e0andr mod qS6=w6+e0anda mod qS7=w7+e0 and a1mod qS8=w8+e0 and a2mod qS9=w9+e0 and b1mod qS10=w10+e0 and b2mod qS11=w11+e0 and r-x1mod qS12=w12+e0 (a-x1+a1) mod qS13=w13+e0, r, and x2mod qS14=w14+e0(a and x2+a2) mod qS15=w15+e0 and r-y1mod qS16=w16+e0(a-y1+b1) mod qS17=w17+e0 and r-y2mod qS18=w18+e0(a-y2+b2) mod q is calculated, and S1-S18, and w0 are sent to other decode person equipments.
Other decode person equipments L=gw0 mod One s1g of pg(s) 2 One s3g of s2=T1 Xe0 modpg(s) 2 s4=T2 Ye0 modpgs5hs6=T3 Re0 modpRs1hs7=T-four e(RX1) 0 modpRs2hs8=T5 e(RX2)0mod pRs3hs9=T6 e(RY1)0mod pRs4hs10 =T7 e(RY2)0mod pgs11 hs12 =T8 e(RX1) 0mod pgs13 hs14 =T9 e(RX2)0mod It verifies that pgs15 hs16 =T10(RY1) e0modpgs17 hs18 =T11(RY2) e0mod plutonium1S11+cS15u2S13+cS17 v-S5=T12Ve0mod p is realized.
0083] Since a top type is realized only when the equipment of Pj creates correctly V, X, Y, R, RX1, RX2, RY1, and RY2, when not realized at least one, it considers verification as failure (explanation which omitted the subscript "j" above). It considers that the equipment of the decode person Pj who failed in certification is a deviation person, and other decode person equipments recover a deviation person's secrecy value x1j', x2j', y1j', y2j', and rj using secrecy value recovery procedure, and it exhibits the value of the right Vj. About secrecy value recovery procedure here, it is reference, for example. A.Herzberg, et.al : "Proactive secret sharing or:How to cope with perpetual leakage", Advances in Cryptology-CRYPTO'95, LNCS 963, pp.339-352, Springer-Verlag, and 1995 It is detailed. The rights (V1, --, Vn) including the value of the exhibited right Vj are obtained.
[0084] After the exponent part of (V1, --, Vn) checks the right thing, the secrecy restoration procedure to exponent part restores a value V. Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop (S8). If equal, each decode person's Pj equipment will calculate Dj=u1zjmodp like the case of drawing 4 . Transmit to all other decode person equipments according to a broadcast mold channel, and each decode person equipment which received Dj verifies the codeword same with having carried out by receiving to (D1, --, Dn) (V1, --, Vn). When injustice is detected, zero information certification is performed similarly, a deviation person is specified, and the value of the right Dj is recovered using secrecy value recovery procedure.
[0085] Zero information certification here is performed as follows. The equipment of Pj chooses a random number d0 from Zq as random, and sends W=g1 and Q=g1 d0 modp to other decode person equipments. Other decode person equipments cooperate and are Rand([c2], [c3]) [W, Q] -> (c2i, c3i) (Ec0, --, Ect).
It performs and Ec0=Wc2QC3 modp is sent to the equipment of Pj.
[0086] The equipment of Pj chooses random numbers d1 and d2 from Zq as random, calculates T12=g1 d1 modpT13=u1d1 modp, and sends it

o other decode person equipments. Other decode person equipments exhibit a distributed secrecy value, recover c2 and c3, and send them to he equipment of Pj.

0087] The equipment of Pj checks that Ec0=Wc2QC3 modp is realized, and when not realized, it stops certification. When this is realized, the quipment of Pj calculates S0=d1+c2 and z1mod q, and sends S0 and d0 to other decode person equipments. Other decode person equipments erify that Q=g1 d0 modpg1 s0=T12Xjc2 modpu1s0=T13Djc2 modp is realized.

0088] Since a top type is realized only when the equipment of Pj creates Dj correctly, when not realized at least one, it considers verification s failure. From the right (D1, --, Dn), with the secrecy restoration procedure to exponent part, each decode person equipment restores D=u1z nod p, calculates m=e/Dmod p, and decodes Message m.

0089] The example of a functional configuration of the decode person equipment in an example 2 is shown in drawing 7 . The private key of :1j, x2j, y1j, y2j, and zj is memorized by memory 21, the open values wj, g1, g2, p, and q etc. are memorized, and since the information further ransmitted to the exterior and the information received from the outside are stored temporarily, memory 21 is used. The distributed random-umber generation section 22 consists of the secrecy distribution machine 23, a distributed secrecy verification machine 24, and a distributed ecrecy adder 25; and private key x1j, x2j, y1j, y2j, and zj are created by these, and the variance rj of a random number r is also generated. The lash Function operation of c=H (u1, u2) is performed about the receiving cipher E with the hash vessel 26, and the operation of Vj=(u1x1 +cy1ju2 x2j+cy2jv-1) rjmod p is performed by the exponentiation computing element 27. The secrecy distribution section 31 consists of a ecrecy distribution machine 32 and a distributed secrecy verification machine 33, and the secrecy value Vj is distributed by Vjk with a with a hreshold [of 2t] verifiable secrecy variational method. the dispersion which the secrecy restoration procedure to the exponent part of Vk is erformed with the exponent part secrecy restoration vessel 34, and uses w1 of D1, --, Dn as a bottom with the BCH codeword verification essel 35 -- it is checked that a logarithm is the codeword of a BCH code. The broadcast mold communication link receiver 36, the broadcast nold communication link transmitter 37, the individual communication link receiver 38, and the individual communication link transmitter 39 re formed, and each part is made to carry out a sequential operation further by the control section 41.

0090] The same number is numbered and shown in the part which corresponds the functional configuration of the decode person equipment sed for an example 3 at drawing 8 with drawing 7 . By the distributed multiplication means 43, value x1j' which distributed the product of a andom number r and a private key x1 with the secrecy variational method of threshold t, same value x2j', y1j', and y2j' are called for. The ertification section 44 consists of the random-number generation machine 45, a exponentiation computing element 46, and **** multiplication nd an adder 47, and it proves that Vj is as a result of [of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj modp] count to other decode persons by zero nformation certification. Verification under zero information certification procedure is performed by the exponentiation computing element 49 nd comparator 51 of the verification section 48.

0091]

Effect of the Invention] Since the justification of a cipher is verified by verifying whether the value which carried out the exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code with the random number with which everyone of a decode person cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the exponentiation, no information about the value in an original verification type is revealed. By proving to a third party that this value was created correctly by zero information certification, it can prove to a third party that the received cipher does not satisfy the original verification type.

[0092] Furthermore, since the value of the verification type before carrying out a exponentiation is not revealed to all the decode person, either, also when not filling a verification type by performing count of carrying out a exponentiation by random numbers, by cooperation of a total-session person by distributed count, Even if there is an inaccurate person in a decode person, since an aggressor can get no profit, he is the safe decode approach with a threshold to the alternative cipher attack.

[0093] Furthermore, since according to another viewpoint of this invention an inaccurate person is specified and a cipher is verified only using just data by making each decode person prove the justification of a count result by zero information certification, it is possible to verify by the computational complexity proportional to several n of a decode person. Moreover, when a right cipher is received by setting the open value of each decode person's proper that each decode person's count result serves as a codeword of a BCH code, and an addressee verifying first that a count result is a codeword, and performing zero information certification only when it is not a codeword, it is possible to perform efficient count, with traffic stopped.

[0094] Furthermore, when other decode persons compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified Although it also becomes bored, even if 1/3 or more inaccurate persons exist by enabling it to calculate a right result instead of the inaccurate decode person, as long as it is less than 1/2, it is possible to obtain a right verification result and a decode result.

[Translation done.]

TECHNICAL FIELD

Field of the Invention] This invention relates to the cipher verification approach that a decode person verifies the justification of a cipher especially, and its program documentation medium, about the safe code approach that the information about a decode person's private key does not leak, also when the content of a communication link is kept secret when communicating by the electrical-communication system, and the content of decode is exhibited.

Translation done.]

NOTICES *

.This document has been translated by computer. So the translation may not reflect the original precisely.
.**** shows the word which can not be translated.
.In the drawings, any words are not translated.

RIOR ART

Description of the Prior Art] In a cryptosystem strong against a selection plaintext attack, a decode person verifies that the transmitting person f a cipher knows the original plaintext by a certain approach. A Cramer-Shoup code Paper R.Cramer and V.Shoup:"A practical public key ryptosystem provablysecure against adaptive chosen Were proposed by chipertext attack", Advances in Cryptology-CRYPTO'98 and LNCS 462, Springer-Verlag, pp.13-25, and 1998. It is the public-key-encryption approach that it can prove that it is strong to an accommodative election cipher attack under an assumption which is called existence of a general purpose one direction nature Hash Function and the difficulty f a Diffie-Hellman judging problem and which is believed widely. A Cramer-Shoup code is the code approach supposing one person's decode erson with one private key corresponding to one public key.

0003] By the Cramer-Shoup code approach that it is already known in the case of the 1 decode person that it is strong to an accommodative election cipher attack First, choose the big prime factors p and q so that q may divide p-1, and the origin g1 and g2 of the subgroup Gq of the rder q of a multiplicative group Zp is used. It is **(x1, x2, y1, y2, z) Zq5 about a private key. A public key is set to 1x1g 2 x2mod p of X=g, y1g2of Y=g y2mod p, and Z=g1z mod p. The cipher E over plaintext m**Gq consists of (u1, u2, v, e), and the cipher created correctly atisfies u1=g1r mod p, u2=g2r mod p, c=H (u1, u2), v=Xr Ycrmod p, and e=mZr mod p to a certain random number r. First, c=H (u1, u2) is alculated and it verifies whether a cipher fills verification type u1x1+cy1u2 x2+cy2**v (mod p), the decode person who received this cipher efuses decode of that cipher, when not filling, when filling, calculates m=e/u1z modp and gets Plaintext m.

0004] By the above-mentioned verification type, a decode person can check that the maker of a cipher knows the original plaintext m. Since lecode is refused to the unjust cipher with which a verification type is not filled, as for an aggressor, information with useful any is not cquired, either. However, when refusing decode by this cipher verification approach as a result of verification, it is actually difficult to prove he information concerning [that the cipher verified to the third party does not serve as V!=v (mod p) as inaccurate / 2 (mod p) /, i.e., V**u1x1+cy1u2 x2+cy, and] V, without leaking information in any way.

0005] Furthermore, by secrecy distribution distributing a corresponding private key to two or more partial private keys to one public key, and naking this hold to two or more decode persons so that it may often be carried out by an ElGamal cryptosystem etc. As opposed to an unjust cipher with which a verification type is not filled in this code decode approach when the decode person of the manpower exceeding a threshold cooperates and it applies the decode with a threshold which enables it to decode a cipher Since the count result V of left part u1x1+cy1u2 x2+cy2 of a verification type becomes known to two or more decode persons, when the decode person who conspired with the aggressor exists, information is revealed to an aggressor and the safety to a selection cipher attack cannot be maintained.

0006] the decode approach with a threshold -- paper V.Shoup and R.Gennaro: "Securing threshold cryptosystems against chosen ciphertext attack", Advances in Cryptology-EUROCRYPT, 98, LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 It is shown under an assumption called existence of random Oracle that the proposed method is strong to an accommodative selection cipher attack.

0007] However, an assumption called random Oracle can obtain no guarantee about the safety, when it is very unreal and random Oracle is eplaced and used for the Hash Function considered that the usual collision is difficult.

Translation done.]

NOTICES *

.This document has been translated by computer. So the translation may not reflect the original precisely.
:.**** shows the word which can not be translated.
..In the drawings, any words are not translated.

:FFECT OF THE INVENTION

Effect of the Invention] Since the justification of a cipher is verified by verifying whether the value which carried out the exponentiation of the 'alue of the verification type at the time of the decode in a Cramer-Shoup code with the random number with which everyone of a decode)erson cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the exponentiation, no information ibout the value in an original verification type is revealed. By proving to a third party that this value was created correctly by zero information :ertification, it can prove to a third party that the received cipher does not satisfy the original verification type.
0092] Furthermore, since the value of the verification type before carrying out a exponentiation is not revealed to all the decode person, either, ilso when not filling a verification type by performing count of carrying out a exponentiation by random numbers, by cooperation of a total- :ession person by distributed count, Even if there is an inaccurate person in a decode person, since an aggressor can get no profit, he is the safe lecode approach with a threshold to the alternative cipher attack.
0093] Furthermore, since according to another viewpoint of this invention an inaccurate person is specified and a cipher is verified only using ust data by making each decode person prove the justification of a count result by zero information certification, it is possible to verify by the :omputational complexity proportional to several n of a decode person. Moreover, when a right cipher is received by setting the open value of :ach decode person's proper that each decode person's count result serves as a codeword of a BCH code, and an addressee verifying first that a :ount result is a codeword, and performing zero information certification only when it is not a codeword, it is possible to perform efficient :ount, with traffic stopped.
0094] Furthermore, when other decode persons compute and exhibit the distributed private key which the inaccurate decode person has in :ooperation with the case where an inaccurate person is specified Although it also becomes bored, even if 1/3 or more inaccurate persons exist)y enabling it to calculate a right result instead of the inaccurate decode person, as long as it is less than 1/2, it is possible to obtain a right /erification result and a decode result.

Translation done.]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] In a Cramer-Shoup code, the object of this invention, without leaking the information about the value in a verification type entirely When the justification of a cipher can be verified and it is shown that the value of a verification type is not just When the decode person of further plurality [prove / for a third party] cooperates and verifies that the value is created correctly by zero information certification, even if there is an inaccurate person in a decode person The value of a verification type is to offer the cipher verification approach which is not revealed to a decode person, either, its program documentation medium, and its equipment.

[Translation done.]

· NOTICES *

MEANS

Means for Solving the Problem] The exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code is carried out with the random number with which everyone of a decode person cannot know the value, and the justification of a cipher is verified by verifying whether the result of having carried out the exponentiation is set to 1. Count of carrying out a exponentiation by these random numbers, by carrying out by cooperation of a total-session person by distributed count Also when not filling a verification type, the value of the verification type before carrying out a exponentiation is revealed to no decode person, and it is got blocked. When not just Since calculated value turns into a value which is not 1 and the exponentiation of the value is carried out by the random numbers, even if the value by which the exponentiation is carried out is shown and it is shown that calculated value is not 1, i.e., are not just, the value in front of the exponentiation is hidden, and there is no possibility that information may leak.
[0010] Setting n persons' decode person to P1-Pn, each decode person Pj (j= 1, 2, --, n) shall have the open value wj of a proper. (x1, x2, y1, y2, z) **Zq5 It distributes with the secrecy variational method of threshold t, and let the secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj be the decode person's Pj private key.
[0011] Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. It considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.
[0012] E= (u1, u2, v, e) is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's Pj equipment acquires the secrecy value rj. Here, rj is a secrecy value corresponding to the value wj at the time of distributing random-number r**Zq with the secrecy variational method of threshold t, and is the value which can recover r with a secrecy decode procedure from the secrecy value of t+1 piece of arbitration. Moreover, each decode person equipment cannot know the value of r, but r becomes the random integer of under or more 0q from the property of a distributed random-number generation procedure.
[0013] The equipment of each decode person Pj who received E calculates c=H (u1, u2) and Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p. Furthermore, Vj is distributed with a with a threshold [of 2t] verifiable secrecy variational method, and the secrecy value Vjk corresponding to a value wk (k= 1, 2, --, n, k!=j) is transmitted through a channel safe for each decode person's Pk equipment. After receiving Vjk from all other decode person equipments, the decode person's Pk equipment transmits Vk to all other decode person equipments through a broadcast mold channel. As for each decode person equipment, each Vk which received verifies using Vkj that it is a right value.
[0014] 2t+1 piece is chosen among the right and checked Vk, and it investigates whether the value V restored with the secrecy restoration procedure to exponent part, i.e., x1k+cy1k, and x2k+cy2k is equal to 1. If not equal, a secrecy restoration procedure will be similarly repeated in other combination, and if a restoration value is all equal to 1 about no 2t+1 piece combination, decode will be refused and it will stop.
[0015] the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right Vk of the arbitration beyond 2t+1 piece -- V=(u1x1+cy1u2 x2+cy2v-1) r mod p -- V can be restored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type u1x1+cy1u2 x2+cy2 in law] v. On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are 1/q, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v, when in cooperation with 1.
[0016] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of ** of making it the value V of the verification type to the just cipher E not set to 1 [or] First, in order to make the object of (1) successful, it must be made for the value of V restored from a certain 2t+1 piece Vk to be set to 1. However, before all decode person equipments including inaccurate person equipment get to know the value of Vk which other decode person equipments take out Since the value of Vk of self-equipment cannot be changed after having to distribute the value of one's Vk by the verifiable secrecy distribution approach and getting to know the value of Vk of other decode person equipments Only when the anticipation about Vk of other decode person equipments comes true, an inaccurate decode person can attain the object of (1). The probabilities for anticipation to come true are 1/q, and since they are small enough, they can be disregarded. Next, since an inaccurate person is at most t persons and, as for other 2t+1 person equipments, the right value is transmitted even if inaccurate decode person equipment transmits what kind of unjust value Vk about the case of (2), the whole of at least one kind can take the set which consists of 2t+1 piece Vk of a right value, and V= 1 is restored from such a set.
[0017] Since one value of r which fills V=(u1x1+cy1u2 x2+cy2v-1) r mod p to any values of u1x1+cy1u2 x2+cy2 about informational leakage when V is not 1 becomes settled Even if the value of (u1x1+cy1u2 x2+cy2v-1) is randomized by r and shows this randomized value, the value before being randomized by r does not leak, that is, the information about u1x1+cy1u2 x2+cy2 does not leak at all by the above-mentioned verification approach.
[0018] As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice

according to this invention is less than [of all decode persons] 1/3, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode equipment strong against an accommodative selection cipher attack can be constituted.

[0019] When n decode persons are in the above technique, to n data for verification (V1, --, Vn) received from all decode person equipments, each decode person equipment takes out 2t+1 piece data, and verifies whether a certain verification type is satisfied. When not satisfied, this verification is performed to all the 2t+1 piece combination that can be taken to n pieces. Therefore, in not satisfying a verification type, it has the fault that computational complexity increases exponentially, to several n of a decode person.

[0020] According to another viewpoint of this invention, in the code decode approach by two or more decode persons, the cipher verification approach and its program documentation medium of a code strong against the accommodative selection cipher attack which can be recovered even if it can perform count efficiently also to many decode persons and 1/3 or more decode persons perform injustice are offered. That is, as a means to reduce the computational complexity to the number of decode persons, by making each decode person equipment prove the justification of that result by zero information certification, an inaccurate person is specified and, according to another viewpoint of this invention, a cipher is first verified only using just data. By doing so, it is possible to verify by the computational complexity proportional to several n of a decode person. However, since there is much traffic, when injustice hardly happens, effectiveness is bad [the zero information certification used in this case]. When a right cipher is received by setting the open value of each decode person's proper that the count result of each decode person equipment serves as a codeword of a BCH code, and addressee equipment verifying that a count result is a codeword, and performing zero information certification only when it is not a codeword, it becomes possible to perform efficient count, with traffic stopped.

[0021] If based on this approach, the number of the inaccurate persons who can approve is to t persons who fill 3t+1>n, and when a safe system with more high tolerance is desired, it is unsuitable. Moreover, although it also becomes bored when an inaccurate person is less than [1/3 or more] 1/2, and other decode person equipments compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified as a means, a technical problem is solved by enabling it to calculate a right result instead of the inaccurate decode person.

[0022] The concrete means is as follows. n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode person Pj. Threshold t which fills 3 t<n is defined. (x1, x2, y1, y2, z) **Zq5 It distributes with the secrecy variational method of threshold t, and let the secrecy value (x2 j and y1 j, y2 x1j, j, zj) corresponding to a value wj be the decode person's Pj private key.

[0023] Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. It considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p (X, Y, Z) for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.

[0024] E= (u1, u2, v, e) is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's Pj equipment acquires the secrecy value rj. Here, rj is a secrecy value corresponding to the value wj at the time of distributing random-number r**Zq with the secrecy variational method of threshold t, and is the value which can recover r with a secrecy decode procedure from the secrecy value of t+1 piece of arbitration. Moreover, each decode person cannot know the value of r, but r becomes the random integer of under or more 0q from the property of a distributed random-number generation procedure.

[0025] Next, all decode person equipments cooperate, and perform a distributed multiplication means, and each decode person's Pj equipment obtains secrecy value x1j', x2j', y1j', and y2j'. Secrecy value x1j' is a value which distributes the product of a random number r and a private key x1 with the secrecy variational method of threshold t, and is acquired, and can decode x1j' to r-x1 (mod q) which t+1 person's decode person of arbitration has here. r and x2 (mod q), r-y1 (mod q), and r-y2 (mod q) can be similarly restored from the value of t+1 piece of arbitration about secrecy value x2j', y1j', and y2j', respectively.

[0026] Each decode person Pj equipment which received E calculates c=H (u1, u2) and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p, and transmits Vj to all other decode person equipments through a broadcast mold channel. Next, each decode person equipment checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code. When it becomes clear not the codeword of a BCH code but that it is not right, the exponent part of (V1, --, Vn) each decode person's Pj equipment It proves to other decode persons by zero information certification, without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj.

[0027] It considers that the decode person Pj who failed in certification is an inaccurate person, and other decode person equipments recover secrecy value x1j' of the deviation person who is the inaccurate person, x2j', y1j', y2j', and rj using secrecy value recovery procedure, and he exhibits the value of the right Vj. The rights (V1, --, Vn) including the value of the exhibited right Vj are obtained. After the exponent part of (V1, --, Vn) checks the right thing and that it is a codeword, the secrecy restoration procedure to exponent part restores a value V. Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop.

[0028] If equal, each decode person's Pj equipment will calculate Dj=u1zjmod p, and will transmit it to all other decode person equipments according to a broadcast mold channel. Each decode person equipment which received Dj verifies the codeword same with having carried out to (V1, --, Vn) to (D1, --, Dn), when injustice is detected, performs zero information certification similarly, specifies an inaccurate person, and it recovers the value of the right Dj using secrecy value recovery procedure.

[0029] From the right (D1, --, Dn), with the secrecy restoration procedure to exponent part, each decode person equipment restores D=u1z mod p, calculates m=e/Dmod p, and decodes Message m. the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right Vk of the arbitration beyond 2t+1 piece -- V= (u1x1+cy1u2 x2+cy2v-1) r mod p -- V can be restored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type u1x1+cy1u2 x2+cy2 in law] v. On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are 1/q, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v, when in cooperation with 1.

[0030] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of ** of making it the value V of the verification type to the just cipher E not set to 1 [or] However, the output of all decode person

:quipments can detect the existence, if an unjust value is less than [of the whole] 1/3 when an unjust value exists since it is verified by :odeword inspection of a BCH code. In such a case, since each decode person proves the rightness of an output value by zero information :ertification, the inaccurate person who outputted the unjust value fails in certification, and is eliminated.
'0031] About informational leakage, when V is not 1, since one value of r which fills V=(u1x1+cy1u2 x2+cy2v-1) r mod p to any values of 11x1+cy1u2 x2+cy2 becomes settled, by the above-mentioned verification approach, the information about u1x1+cy1u2 x2+cy2 does not leak it all. As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according o this invention is less than [of all decode persons] 1/3, by cooperation of two or more decode person, it is possible to calculate a verification ype equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode ipproach strong against an accommodative selection cipher attack can be constituted.
.0032] By computing and exhibiting the distributed private key which codeword inspection of a BCH code is not conducted, but zero nformation certification is always performed in the above-mentioned means on the other hand, an inaccurate person is specified, other decode)ersons cooperate, and the inaccurate decode person has Although it also becomes bored, since a right result is calculable instead of the naccurate decode person, it can respond to less than 1/2 inaccurate person (in order to determine by majority that zero information certification .s right, one half of decode persons at least must be right).
'0033]
'Embodiment of the Invention] The cipher verification approach which is the first example of this invention is explained to one or less :xample. The cipher created with cipher implementer equipment 11 as shown in drawing 1 is decoded with decode person equipment 12. If it is iot a right cipher, in order to avoid carrying out decode refusal freely with decode person equipment 12, it verifies whether decode refusal is ippropriate with verification person equipment 13.
[0034] There shall be the big prime factors p and q now, and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. It considers as :he public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p for an encryption procedure. Here, it is **(x1, x2, y1, y2, z) Zq5. It carries out. The public key shall be exhibited with p, q, g1, and g2 as a open parameter. Moreover, the private key shall be stored on the memory of decode person equipment.
[0035] As shown in drawing 2 , after receiving cipher E= (u1, u2, v, e) of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y, and Z as the public key (S1), Decode person equipment generates a random number r (S2), and calculates c=H (u1, u2) and V=(u1x1+cy1u2 x2+cy2v-1) r mod p (S3). If V becomes one, this cipher will be considered as acceptance and (S4) and decode count will be performed (S5).
[0036] If V is not 1, it will consider as a rejection. In order to prove that it is a rejection to a third party, BC (r) is exhibited using bit :ommitment function BC(). There are some which are depended on Pedersen in this bit commitment function. That is, a random number s is generated and it calculates with BC(r, s):=gr hs mod p. dispersion of h to which g and h use g as a bottom here -- it is under Gq whose logarithm is strange.
[0037] r which constitutes BC (r, s), x1 which constitutes public keys X and Y, x2, and y1 and y2 -- using -- r mod p (u1x1+cy1u2 x2+cy2v-1) -- it proves to a third party by zero information certification, without leaking the secrecy concerning [that the result of having calculated is V, and] r, x1, x2, and y1 and y2 (S6). [then,] The following procedures perform this zero information certification.
[0038] dispersion of h which uses g as a bottom for g and h below -- it considers as the origin of Gq whose logarithm is strange. decode person equipment -- random numbers a, a1, a2, b1, and b2 -- Zq -- choosing -- R=gr ha mod pRX1=Rx1ha1 modpRX2=Rx2ha2 modpRY1=Ry1hb1 modpRY2=Ry2hb2 modp -- R, RX1, RX2, RY1, and RY2 are sent to verification person equipment.
[0039] Furthermore, decode person equipment chooses a random number w0 from Zq as random, and is K=g and L=gw0. mod p is sent to verification person equipment. Verification person equipment calculates B=Ke0Le1 modp by choosing e0 and e1 from Zq as random, and sends B to decode person equipment.
[0040] Decode person equipment chooses random numbers w1-w18 from Zq as random. T1 =g1 w1g2 w2 mod pT2 =g1 w3g2 w4 mod pT3 =gw5gw6 mod pT4 = Rw1hw7 mod pT5 =Rw2hw8 mod pT6 =Rw3hw9 mod pT7 =Rw4hw10 mod pT8 = Calculate gw11 hw12 mod pT9 =gw13 hw14 mod pT10=gw15 hw16 mod pT11=gw17 hw18 mod pT12=u1w11+cw15u2w13+cw17 v-w5 mod p. It sends to verification person equipment.
[0041] Verification person equipment sends e0 and e1 to decode person equipment.
Decode person equipment checks that B=Ke0Le1 modp is realized, and when not realized, it stops certification. When this is realized, Decode person equipment is z1=w1+e0 and x1 modqz2=w2+e0 and x2 modqz3=w3+e0 and y1 modqz4=w4+e0 and y2 modqz5=w5+e0 and r. modqz6=w6+e0anda modqz7=w7+e0 and a1 modqz8=w8+e0 and a2 modqz9=w9+e0 and b1 modqz10=w10+e0 and b2 modqz11=w11+e0 and r-x1 modqz12=w12+e0 (a-x1+a1) modqz13=w13+e0, r, and x2 modqz14=w14+e0 (a and x2+a2) modqz15=w15+e0 and r-y1 modqz16=w16+e0 (a-y1+b1) modqz17=w17+e0 and r-y2 modqz18=w18+e0 (a-y2+b2) modq It calculates and z1-z18, and w0 are sent to verification person equipment.
[0042] Verification person equipment L=gw0 modpg1 z1g2 z2=T1 Xe0mod pg1 z3g2 z4=T2 Ye0mod pgz5hz6=T3 Re0 modpRz1hz7=T-four e(RX1)0mod pRz2hz8=T5 e(RX2)0mod pRz3hz9=T6 e(RY1)0mod pRz4hz10 =T7 e(RY2)0mod pgz11 hz12 =T8 e(RX1)0mod pgz13 hz14 =T9 e(RX2)0mod It verifies that pgz15 hz16 =T10(RY1) e0mod pgz17 hz18=T11(RY2) e0mod plutonium1z11+cz15u2z13+cz17 v-z5 =T12Ve0mod p is realized.
[0043] The principle of the upper certification is Schnorr. It is the same as that of a signature, and since a verification type is realized only when decode person equipment creates correctly V, X, Y, R, RX1, RX2, RY1, and RY2, when at least one is not realized, verification is considered as failure.
The second example of this invention is explained to two or less example. As shown in drawing 3 R> 3, they are code implementer equipment 11 and 121-12n of each equipment of the decode persons P1-Pn. It connects with the broadcast mold channel 14, and is 121-12n of decode person equipment. It connects by the channel 15 safe for mutual.
[0044] There shall be the big prime factors p and q now, and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. First, n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode person Pj (j= 1, 2, --, n). Threshold t which fills 3 t<n is defined. All decode person equipments perform the distributed random-number generation procedure of threshold t 3 times, and the decode person's Pj equipment acquires a secrecy value (x2 j and y1 j, y2 x1j, j, zj), and makes this the decode person's Pj private key.

Moreover, let Xj=g1x1j g2 x2j mod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. Furthermore, it considers as the public key which uses 1x1g 2 x2mod p of X=g, 1y1g2of Y=g y2mod p, and Z=g1z mod p for an encryption procedure. Here, it is **(x1, x2, y1, y2, z) Zq5. It is the random number restored by the secrecy restoration procedure from t+1 set of secrecy values (x2 j and y1 j, y2 x1j, j, zj) of arbitration. There is an approach by Pedersen in the distributed random-number generation procedure which generates such a random number. Below, the distributed random-number generation procedure is shown.

[0045] Between each decode person equipment, as shown in drawing 3 , there shall be a safe channel 15 and each decode person equipment shall use the broadcast mold channel 14 it is guaranteed to be to receive a content with other all the members' same decode person equipment.

S-1) the equipment of Pj -- two polynomials on Zq -- f(X) =a0 j+a1jX+--+atjXt And gj (X) =b0 j+b1jX+--+btjXt random -- choosing -- every -- fj (wk) and gj (wk) are transmitted to the equipment except for 1, 2, --, n, and k=j k= -- of Pk through a safe channel.

[0046] S-2) The equipment of Pj calculates Cij=g1aij g2bij mod p to i= 1, --, t, and transmits it to all other decode person equipments through a broadcast mold channel.

S-3) The equipment of Pk which received Cij from all other decode person equipments is g1fj(wk) g2gj(wk) =C0jwk0 and C1jwk1 as wki=wki mod q. -- It verifies that Ctjwkt mod p is realized.

[0047] S-4) The equipment of Pk is x1 k=f1(wk)+f2(wk)+. -- They are +fn(wk) mod q and x2k=g1(wk)+g2(wk)+. -- Distributed random-number value x1k and x2k are obtained as +gn(wk) mod q.

S-5) X=C00, C01 -- It is referred to as C0n modp. Private key y1j, y2j, and zj to which public keys Y and Z and each decode person correspond similarly are also created similarly.

[0048] All decode person equipments generate distributed random-number r**Zq with a distributed random-number generation procedure, and each decode person's Pj equipment holds the secrecy value rj (drawing 5 , S1). After receiving cipher E= (u1, u2, v, e) of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y, and Z as the public key (S2), each decode person's Pj equipment calculates c=H (u1, u2) and Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p (S3).

[0049] Then, the equipment of Pj distributes Vj with a with a threshold [of 2t] verifiable secrecy variational method, and the secrecy value Vjk corresponding to a value wk is transmitted through a channel safe for each decode person's Pk equipment (S4). The approach of Pedersen can be used for the verifiable secrecy variational method used here. The following is the procedure.

P-1) g and h which there are the big prime factors P and Q, and Q divides P-1, and are made into Q>p are GQ whose value of log g h is strange. It considers as origin.

[0050] P-2) the equipment of Pj -- ZQ Two upper polynomials fj (X) =Vj+a1jX+--+atjXt And gj (X) =b0 j+b1jX+--+btjXt (however, it considers as a0 j=Vj) -- the part of Vj -- removing -- random -- choosing -- every -- fj (wk) and gj (wk), i.e., Vjk, are transmitted to the equipment of Pk through a safe channel.

P-3) The equipment of Pj calculates Cij=gaij hbij mod p to i= 1, --, t, and transmits it to all other decode person equipments through a broadcast mold channel.

[0051] P-4) The equipment of Pk which received Cij is gfj(wk) hgj(wk) =C0jwk0 and C1jwk1 as wki=wki mod q. -- It verifies that Ctjwkt mod p is realized, that is, Vjk is verified (S5).

P-5) When not realized, the equipment of Pk transmits a "rejection" to all other decode person equipments through a broadcast mold channel.

[0052] When advice of P-6 "a rejection" is t+1 or more pieces, it is considered that Pj is an inaccurate person, it is eliminated (S6), and all other decode person equipments discard all the information that the equipment of Pj transmitted before. The step of P-4, and 5 and 6 is the procedure of performing verification of the distributed secrecy value Vjk, and an inaccurate person's abatement, and after all decode person equipments finish transmitting data, you may carry out by releasing a rejection list collectively.

[0053] After all decode person equipments distribute Vj with the above-mentioned procedure, each decode person's Pj equipment transmits Vj and b0j to all other decode person equipments through a broadcast mold channel (S7). The equipment of each decode person Pj who received this checks that C0 j=g1Vjhb0j mod p is realized, and verifies Vj (S8). When not realized, like the above, a "rejection" is notified to all other decode person equipments, and an inaccurate person is eliminated (S9).

[0054] 2t+1 piece is chosen as arbitration from the right and all checked Vk(s) (S10), and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1 (S11). The secrecy restoration procedure to exponent part is reference. Cramer, et.al: "A seure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed. The restoration procedure to the exponent part at the time of setting to alpha the set of the index k of 2t+1 piece Vk chosen as below is shown. The secrecy value of exponent part presupposes that it is the secrecy value acquired with the verifiable secrecy variational method of Pedersen.

[0055] R-1) It is a Lagrange interpolation multiplier first [0056]

[Equation 1]

$$\lambda_{j,\alpha} = \Pi_{k \in \alpha,\ k \neq j}\, j/(j-k)$$

It calculates by carrying out.

R-2) Next, [0057]

[Equation 2]

$$V = \Pi_{j \in \alpha}\ V_j^{\lambda j,\alpha} \mod p$$

It calculates. If V is not 1, a secrecy restoration procedure will be similarly repeated in other 2t+1 piece combination (S12). If a restoration value is all equal to 1 about no combination, a rejection will be notified and it will stop.

[0058] If there is combination set to 1 at least one, this cipher will be considered as acceptance. Each decode person's Pj equipment calculates Dj=u1zjmod p, as shown in drawing 4 R> 4 (S1), and it transmits it to all other decode person equipments according to a broadcast mold channel (S2). the dispersion to which each decode person equipment which received Dj uses u1 of D1, --, Dn as a bottom -- by checking that a logarithm is the codeword of a BCH code, if it is (S4) and a codeword, the secrecy restoration procedure to the above-mentioned exponent part will restore D=u1z mod p (S5), m=e/D modp will be calculated, and Message m will be decoded (S6). If it is not a codeword in step S4, what is made to prove the rightness of count and cannot be proved by zero information certification will be discarded as inaccurate Di (S7).

The third example of this invention is explained to three or less example.
[0059] A safe channel shall be between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment. There shall be the big prime factors p and q and q shall divide p-1. The origin g1 and g2 of Gq is chosen at random. First, n persons' decode person is set to P1-Pn, and the open value wj of a proper is assigned to each decode person Pj. Threshold t which fills 3 t<n is defined.
[0060] First, the secrecy distribution approach by Pedersen is shown. First, g and h It considers as the origin of Gq whose logg h is strange. The equipment of the portioner P who distributes the secrecy values a0 and b0 is t-th two polynomials f(X) =a0+a1X+ on Zq. -- It is +atXt and g(X) =b0+b1X+. -- It is +btXt. Except for a0, it chooses at random, and f (wj) and g (wj) are sent to each addressee's Pj equipment through a safe channel.
[0061] Next, the commitment value Ei of each multiplier is calculated like Ei=gaihbimod p to i= 0, --, t, and it opens to the public through a broadcast mold channel. Each equipment of Pj which received these is gf (wj) as uji=wji mod q. hg (wj) =E0uj0 E1uj1 -- It verifies that Etujt mod p is realized. This E0uj0 E1uj1 -- The value of Etujt mod p is called the commitment to the distributed secrecy value of Pj. If the commitment value of each multiplier is exhibited, anyone can also calculate the commitment to which distributed secrecy value of Pj.
[0062] Below, it is Ped (a0, b0) about this secrecy distribution approach [g, h]. -> (a0j, b0j) (E0, --, Et)
** -- it writes like. (a0, b0) are confidential information distributed, each equipment of Pj is the distributed secrecy value received through a safe channel, and its (a0j, b0j) are equal to f (wj) and g (wj) respectively. (E0, --, Et) are commitment values of each multiplier exhibited through a broadcast mold channel. [g, h] express the bottom used in case a commitment is created. As long as there is especially no notice about the above-mentioned notation, the multiplier of the polynomial except a constant term shall be chosen at random.
[0063] Thus, from the distributed secrecy value, when polynomial interpolation recovers the original secrecy, the holder of each distributed secrecy value exhibits the value first. It is ga0j hb0j =E0uj0 E1uj1 to the exhibited value (a0j, b0j). -- It checks that Etujt modp is realized. The set which that index j makes is set to alpha about t+1 (a0j, b0j) of arbitration of which this formula consists. It is a Lagrange interpolation multiplier [0064]
[Equation 3]
$$\lambda_{i,\alpha} = \Pi_{k \in \alpha,\ k \neq i}\ i/(i-k) \bmod q$$

It is [0065] when it carries out.
[Equation 4]
$$\sum_{j \in \alpha} \lambda_{i,\alpha}\ a0j \bmod q = a0$$

A next door and a0 are recoverable. b0 is recoverable similarly. The above-mentioned secrecy distribution approach can completely be similarly performed, even if it uses only one bottom. In such a case, it is written as Ped(a0) [g] -> (a0j) (E0, --, Et).
[0066] The random number distributed in cooperation by two or more persons is generable using this secrecy distribution approach. First, the equipment of Pi chooses random numbers ai and bi from Zq, and is this Ped(ai, bi) [g, h] -> (aij, bij) (Ei0, --, Eit)
** -- it distributes like. All the members of P1-Pn perform this. Then, the equipment of Pj receives (a1j, b1j), --, (anj, bnj) from a safe channel, and receives (E10, --, E1t), --, (En0, --, Ent) from a broadcast mold channel. At this time, it is the distributed secrecy value (x1j, x2j) of Pj x1j=a1j+ -- +anj modq, x2j=b1j+ -- It is referred to as +bnj modq. The random-number value x1 recovered from this distributed secrecy value is [0067].
[Equation 5]
$$x1 = \sum_{j \in \alpha} \lambda_{k,\alpha}\ x1j = a1 + \cdots + an \bmod q$$

The value is known by nobody until it comes out, and it is and recovery is performed. Moreover, the commitment value EXk of the k-th multiplier of the polynomial which makes this secrecy random-number value a constant serves as EXk=E1 k-E2 k--Enkmod p. Especially, it is cautious of it being EX0=gx1hx2mod p. This approach is called distributed random-number generation, and it is Rand([a], [b]) [g, h] -> (aj, bj) (E0, --, Et).
It writes. ([a] [b]) is a random-number value generated and means that the value of [ ] is strange to every calculator. [g, h] -- and [of semantics] (aj, bj) (E0, --, Et) is the same as that of the notation of the above-mentioned secrecy distribution.
[0068] All decode person equipments are the distributed random-number generation procedure of threshold t Rand([x1], [x2]) [g1, g2] -> (x1j, x2j) (EX0, --, EXt)
Rand([y1], [y2]) [g1, g2] -> (y1j, y2j) (EY0, --, EYt)
Rand ([z1]) [g1] -> (z1j) (EZ0, --, EZt)
** -- performing 3 times like, the decode person Pj acquires a secrecy value (x2 j and y1 j, y2 x1j, j, zj), and makes this the decode person's Pj private key. Moreover, let Xj=g1x1j g2 x2jmod p, Yj=g1y1j g2y2j mod p, and Zj=g1zjmod p (Xj, Yj, Zj) be the decode person's Pj public keys. Furthermore, it considers as the public key which uses X=EX0=g1x1g2 x2modp, Y=EY0=g1y1g2y2mod p, and Z=EZ0=g1z mod p for an encryption procedure. It is **(x1, x2, y1, y2, z) Zq5 here. It is the random number restored by the secrecy restoration procedure from t+1 set of secrecy values (x2 j and y1 j, y2 x1j, j, zj) of arbitration.
[0069] All decode person equipments perform distributed random-number generation procedure Rand ([r], [s]) [g1, g2] -> (rj, sj) (R0, --, Rt), and generate distributed random-number r**Zq, and each decode person's Pj equipment holds the secrecy values rj and sj (drawing 6 , S1). R is set to R=R0=g1r g2second mod p here.
[0070] Next, all decode person equipments obtain secrecy value x1j', x2j', y1j', and y2j' with a distributed multiplication means (S2). Secrecy value x1j' is a value which distributes the product of a random number r and a private key x1 with the secrecy variational method of threshold t, and is acquired, and can decode rx1 (mod q) here from x1j' which t+1 person's decode person of arbitration has. rx2 (mod q), ry1 (mod q), and ry2 (mod q) can be similarly restored from the value of t+1 piece of arbitration about secrecy value x2j', y1j', and y2j', respectively. About such a distributed multiplication means, it performs as follows.
[0071] The decode person's Pj equipment is Ped(x1j, x2j) [g1, g2] -> (x1ji, x2 ji) (EXj0, --, EXjt).
It performs. Each equipment of Pj calculates Rj=g1rjg2sjmod p. This value Rj is Rj=R0uj0 R1uj1 as uji=wji mod q. -- Since you may calculate

ike Rtujt mod p, it is cautious of the ability of anyone to calculate.
0072] Next, the polynomial used for distributing x1j and x2j by Ped (x1j, x2j) is used for the equipment of Pj as it is, and it is Ped(x1j, s1j) Rj, g2] -> (x1ji, s1ji) (ERX 1j0, --, ERX1jt).
ed(x2j, s2j) [Rj, g2] -> (x1ji, s2ji) (ERX 2j0, --, ERX2jt)
t performs. However, s1j and s2j also choose at random the polynomial which chooses at random and makes these a constant term.
0073] To the last, the equipment of Pj is Ped(x1 j-rj, x1j-sj+s1j) [g1, g2] -> (rx1ji, rs1ji) (ERX 1j0, --, ERX1jt).
ed(x2j-rj, x2j-sj+s2j) [g1, g2] -> (rx2ji, rs2ji) (ERX 2j0, --, ERX2jt)
t carries out.
0074] Each equipment of P1-Pn performs the above-mentioned procedure. The equipment of Pi is the set (rx11i, --, rx1ni) of a distributed ecrecy value which received to a Lagrange interpolation multiplier [0075]
Equation 6]
$\lambda_{j,\alpha} = \Pi_{k\in\alpha,\ k\neq j}\, j/(j-k)$ として、

$$x1j' = \sum_{j\in\alpha}\lambda_{j,\alpha}\, rx1ji \mod q$$

t calculates. The set of the index of right x1j' is set to beta, and it is [0076] at the time of |beta|>=t+1.
Equation 7]

$$\sum_{j\in\beta}\lambda_{j,\beta}\, x1j' = \sum_{j\in\beta}\{\lambda_{j,\beta}\sum_{j\in\alpha}\lambda_{i,\alpha}\, rx1ij\}$$

$$= \sum_{i\in\alpha}\lambda_{i,\alpha}\{\sum_{j\in\beta}\lambda_{j,\beta}\, rx1ij\}$$

$$= \sum_{i\in\alpha}\lambda_{i,\alpha}\, ri\cdot x1i = r\cdot x1$$

Since a next door and multiplication result r-x1 are recoverable, it turns out that x1j' is the t-th distributed secrecy value of r-x1. x2j' as well as x1j' is calculated. Furthermore, a distributed multiplication procedure is similarly performed and calculated about secrecy value y1j' and y2j'.
0077] After receiving cipher E= (u1, u2, v, e) to the plaintext m enciphered by the Cramer-Shoup code approach (S3), each decode person's Pj equipment c=H (u1, u2) and Vj=u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p are calculated, and Vj is transmitted to all other decode person equipments through (S4) and a broadcast mold channel (S5). Next, as for each decode person equipment, the exponent part of (V1, --, Vn) checks that it is the codeword of a BCH code (S6). A codeword verification procedure reference F.J.MacWilliams : "The Thory of Error Correcting Codes", North-Holland Mathematical Library, and pp.201-202 -- or M. Ben-Or and S.Goldwasser, A. Wigerson:" Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation" and 20 th ACM Symposium on Theory It is detailed to of Computing, pp.1-10, and 1988. A codeword verification procedure is shown below.
- w!=1 is used as the n-th root of 1 in mod q, and it is referred to as xiij=wj (i-1) modq.
- It is [0078] about j= 1, --, all 2t j.
[Equation 8]

$$V_1^{\xi 1j}\, V_2^{\xi 2j}\cdots V_n^{\xi nj} \mod p = 1$$

It checks becoming. When it becomes clear with the above-mentioned procedure that the exponent part of (V1, --, Vn) is not right, each decode person's Pj equipment It proves to other decode person equipments by zero information certification, without leaking the information concerning [that Vj is as a result of / of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj mod p / count, and] x1j', x2j', y1j', y2j', and rj (S7).
[0079] This zero information certification is performed as follows. However, by explanation of the procedure to following Pj, since Subscript j is attached to all variables, this is excluded and explained. First, distributed secrecy value x1' which Pj holds, x2', y1', y2', and r are received. a, a1, a2, and b1 as a certain random number R=g1r g2second mod pRX1=ERX10=Rx1g2a1mod pRX2=ERX20=Rx2g2a2mod pRY1=ERY10=Ry1g2b1mod pRY2=ERY20=Ry2g2b2mod The values R, RX1, RX2, RY1, and RY2 of a commitment p Becoming can be acquired from the commitment value of the multiplier exhibited with the distributed random-number generation means and the distributed multiplication means to anyone.
[0080] Pj chooses a random number w0 from Zq as random, and sends K=g and L=gw0mod p to other decode person equipments. Other decode person equipments cooperate and are Rand([e0], [e1]) [K, L] -> (e0i, e1i) (Ee0, --, Eet).
It performs and Ee0=Ke0Le1mod p is sent to the equipment of Pj.
[0081] The equipment of Pj chooses random numbers w1-w18 from Zq as random. T1 =g1w1g2 w2 modpT2 = g1 w3g2 w4 modpT3 =gw5gw6 modpT4 =Rw1hw7 modpT5 = Rw2hw8 modpT6 =Rw3hw9 modpT7 =Rw4hw10modpT8 = Calculate gw11 hw12 mod pT9 =gw13 hw14 mod pT10=gw15 hw16 mod pT11=gw17 hw18 mod pT12=u1w11+cw15u2w13+cw17 v-w5 modp. It sends to other decode person equipments.
[0082] Other decode person equipments exhibit a distributed secrecy value, recover e0 and e1, and send them to the equipment of Pj. The equipment of Pj checks that Ee0=Ke0Le1 modp is realized, and when not realized, it stops certification. When this is realized, The equipment of Pj S1=w1+e0 and x1mod qS2=w2+e0andx2mod qS3=w3+e0andy1mod qS4=w4+e0andy2mod qS5=w5+e0andr mod qS6=w6+e0anda mod qS7=w7+e0 and a1mod qS8=w8+e0 and a2mod qS9=w9+e0 and b1mod qS10=w10+e0 and b2mod qS11=w11+e0 and r-x1mod qS12=w12+e0 (a-x1+a1) mod qS13=w13+e0, r, and x2mod qS14=w14+e0(a and x2+a2) mod qS15=w15+e0 and r-y1mod qS16=w16+e0(a-y1+b1) mod qS17=w17+e0 and r-y2mod qS18=w18+e0(a-y2+b2) mod q is calculated, and S1-S18, and w0 are sent to other decode person equipments. Other decode person equipments L=gw0 mod One s1g of pg(s) 2 One s3g of s2=T1 Xe0 modpg(s) 2 s4=T2 Ye0 modpgs5hs6=T3 Re0 modpRs1hs7=T-four e(RX1) 0 modpRs2hs8=T5 e(RX2)0mod pRs3hs9=T6 e(RY1)0mod pRs4hs10 =T7 e(RY2)0mod pgs11 hs12 =T8 e(RX1) 0mod pgs13 hs14 =T9 e(RX2)0mod It verifies that pgs15 hs16 =T10(RY1) e0modpgs17 hs18 =T11(RY2) e0mod plutonium1S11+cS15u2S13+cS17 v-S5=T12Ve0mod p is realized.

0083] Since a top type is realized only when the equipment of Pj creates correctly V, X, Y, R, RX1, RX2, RY1, and RY2, when not realized at east one, it considers verification as failure (explanation which omitted the subscript "j" above). It considers that the equipment of the decode ›erson Pj who failed in certification is a deviation person, and other decode person equipments recover a deviation person's secrecy value x1j', :2j', y1j', y2j', and rj using secrecy value recovery procedure, and it exhibits the value of the right Vj. About secrecy value recovery procedure ıere, it is reference, for example. A.Herzberg, et.al : "Proactive secret sharing or:How to cope with perpetual leakage", Advances in Cryptology-CRYPTO'95, LNCS 963, pp.339-352, Springer-Verlag, and 1995 It is detailed. The rights (V1, --, Vn) including the value of the :xhibited right Vj are obtained.

0084] After the exponent part of (V1, --, Vn) checks the right thing, the secrecy restoration procedure to exponent part restores a value V. Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop (S8). If equal, each lecode person's Pj equipment will calculate Dj=u1zjmodp like the case of drawing 4 . Transmit to all other decode person equipments ıccording to a broadcast mold channel, and each decode person equipment which received Dj verifies the codeword same with having carried ›ut by receiving to (D1, --, Dn) (V1, --, Vn). When injustice is detected, zero information certification is performed similarly, a deviation ›erson is specified, and the value of the right Dj is recovered using secrecy value recovery procedure.

0085] Zero information certification here is performed as follows. The equipment of Pj chooses a random number d0 from Zq as random, and ;ends W=g1 and Q=g1 d0 modp to other decode person equipments. Other decode person equipments cooperate and are Rand([c2], [c3]) [W, Q] -> (c2i, c3i) (Ec0, --, Ect).

It performs and Ec0=Wc2QC3 modp is sent to the equipment of Pj.

0086] The equipment of Pj chooses random numbers d1 and d2 from Zq as random, calculates T12=g1 d1 modpT13=u1d1 modp, and sends it :o other decode person equipments. Other decode person equipments exhibit a distributed secrecy value, recover c2 and c3, and send them to :he equipment of Pj.

0087] The equipment of Pj checks that Ec0=Wc2QC3 modp is realized, and when not realized, it stops certification. When this is realized, the :quipment of Pj calculates S0=d1+c2 and z1mod q, and sends S0 and d0 to other decode person equipments. Other decode person equipments verify that Q=g1 d0 modpg1 s0=T12Xjc2 modpu1s0=T13Djc2 modp is realized.

0088] Since a top type is realized only when the equipment of Pj creates Dj correctly, when not realized at least one, it considers verification ıs failure. From the right (D1, --, Dn), with the secrecy restoration procedure to exponent part, each decode person equipment restores D=u1z nod p, calculates m=e/Dmod p, and decodes Message m.

0089] The example of a functional configuration of the decode person equipment in an example 2 is shown in drawing 7 . The private key of x1j, x2j, y1j, y2j, and zj is memorized by memory 21, the open values wj, g1, g2, p, and q etc. are memorized, and since the information further transmitted to the exterior and the information received from the outside are stored temporarily, memory 21 is used. The distributed random-number generation section 22 consists of the secrecy distribution machine 23, a distributed secrecy verification machine 24, and a distributed secrecy adder 25, and private key x1j, x2j, y1j, y2j, and zj are created by these, and the variance rj of a random number r is also generated. The Hash Function operation of c=H (u1, u2) is performed about the receiving cipher E with the hash vessel 26, and the operation of Vj=(u1x1 j+cy1ju2 x2j+cy2jv-1) rjmod p is performed by the exponentiation computing element 27. The secrecy distribution section 31 consists of a secrecy distribution machine 32 and a distributed secrecy verification machine 33, and the secrecy value Vj is distributed by Vjk with a with a threshold [of 2t] verifiable secrecy variational method. the dispersion which the secrecy restoration procedure to the exponent part of Vk is performed with the exponent part secrecy restoration vessel 34, and uses w1 of D1, --, Dn as a bottom with the BCH codeword verification vessel 35 -- it is checked that a logarithm is the codeword of a BCH code. The broadcast mold communication link receiver 36, the broadcast mold communication link transmitter 37, the individual communication link receiver 38, and the individual communication link transmitter 39 are formed, and each part is made to carry out a sequential operation further by the control section 41.

[0090] The same number is numbered and shown in the part which corresponds the functional configuration of the decode person equipment used for an example 3 at drawing 8 with drawing 7 . By the distributed multiplication means 43, value x1j' which distributed the product of a random number r and a private key x1 with the secrecy variational method of threshold t, same value x2j', y1j', and y2j' are called for. The certification section 44 consists of the random-number generation machine 45, a exponentiation computing element 46, and **** multiplication and an adder 47, and it proves that Vj is as a result of [of u1x1j'+cy1j'u2x2j'+cy2 j'v-rj modp] count to other decode persons by zero information certification. Verification under zero information certification procedure is performed by the exponentiation computing element 49 and comparator 51 of the verification section 48.

[Translation done.]

DESCRIPTION OF DRAWINGS

Brief Description of the Drawings]
[Drawing 1] Drawing showing the system configuration of the example 1 of this invention.
[Drawing 2] The flow chart showing the verification operations sequence of the decode person equipment in the example 1 of this invention.
[Drawing 3] Drawing showing the system configuration of the example 2 of this invention.
[Drawing 4] The flow chart showing the decode operations sequence of the decode person's Pi equipment in the example 2 of this invention.
[Drawing 5] The flow chart showing the verification operations sequence of the decode person's Pi equipment in the example 2 of this invention.
[Drawing 6] The flow chart showing the verification operations sequence of the decode person's Pi equipment in the example 3 of this invention.
[Drawing 7] Drawing showing the functional configuration of the decode person equipment in an example 2.
[Drawing 8] Drawing showing the functional configuration of the decode person equipment in an example 3.

[Translation done.]

NOTICES *

.This document has been translated by computer. So the translation may not reflect the original precisely.
.**** shows the word which can not be translated.
.In the drawings, any words are not translated.

DRAWINGS

Drawing 1]

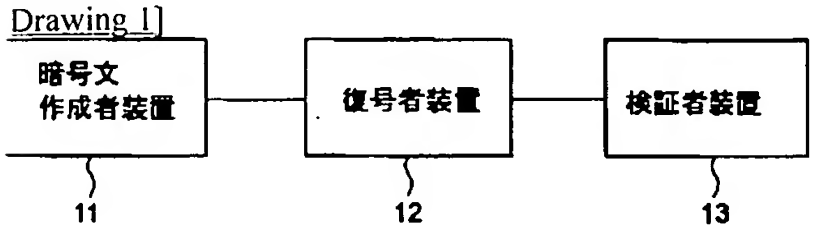

図 1

Drawing 2]

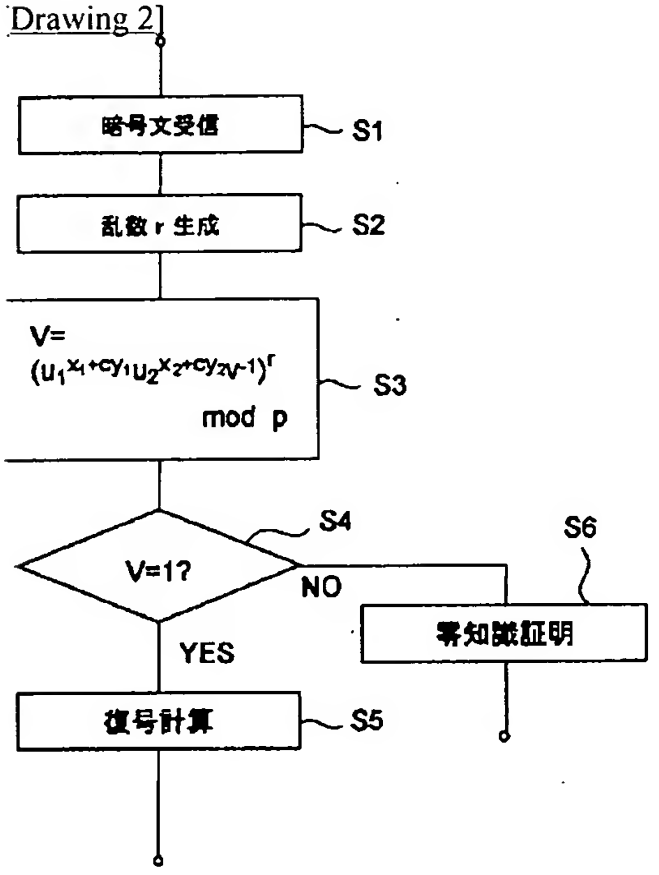

図 2

[Drawing 3]

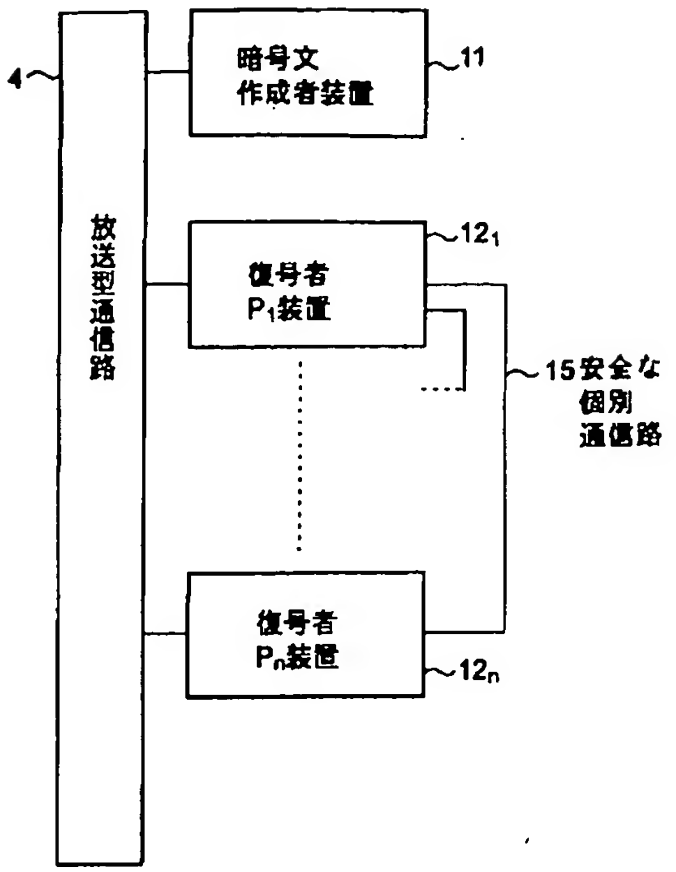

図 3

[Drawing 4]

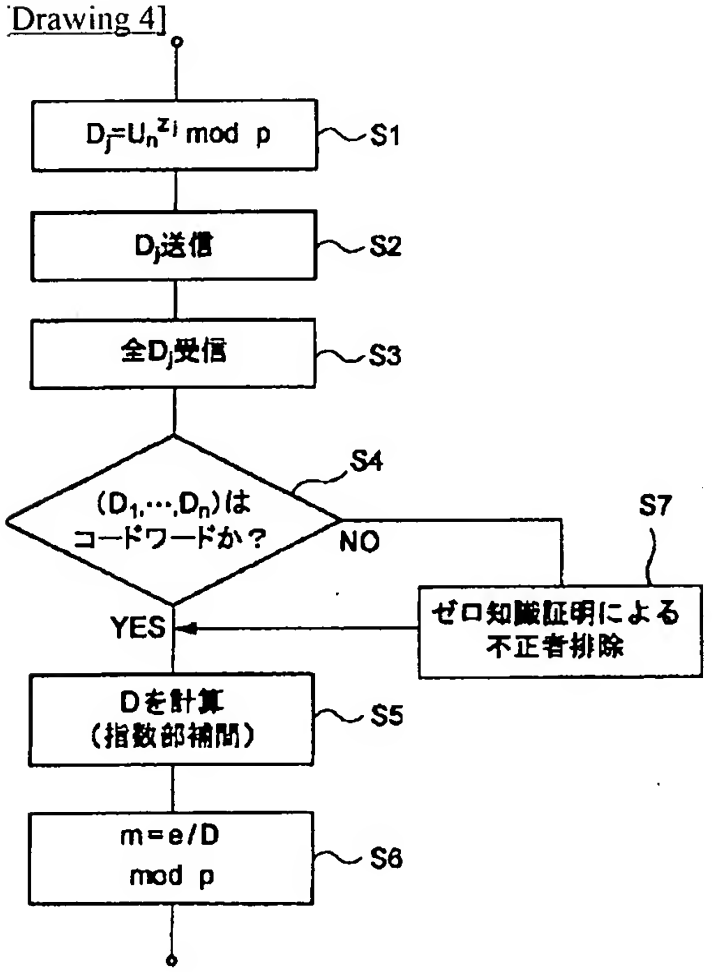

図 4

[Drawing 5]

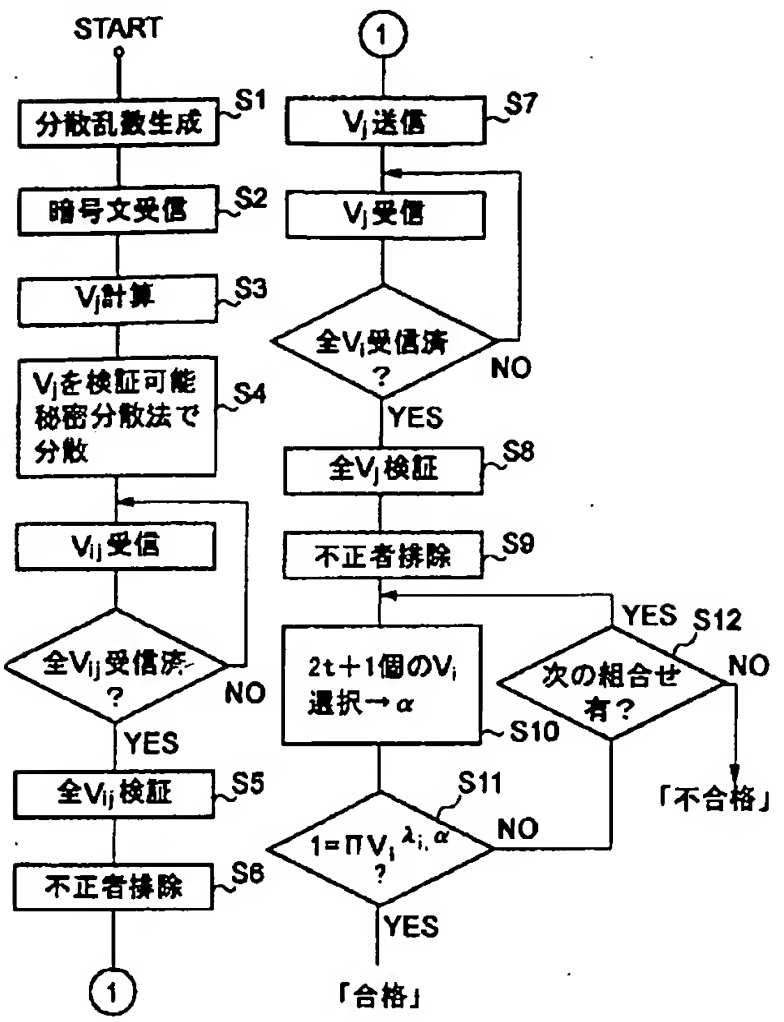

図 5

[Drawing 6]

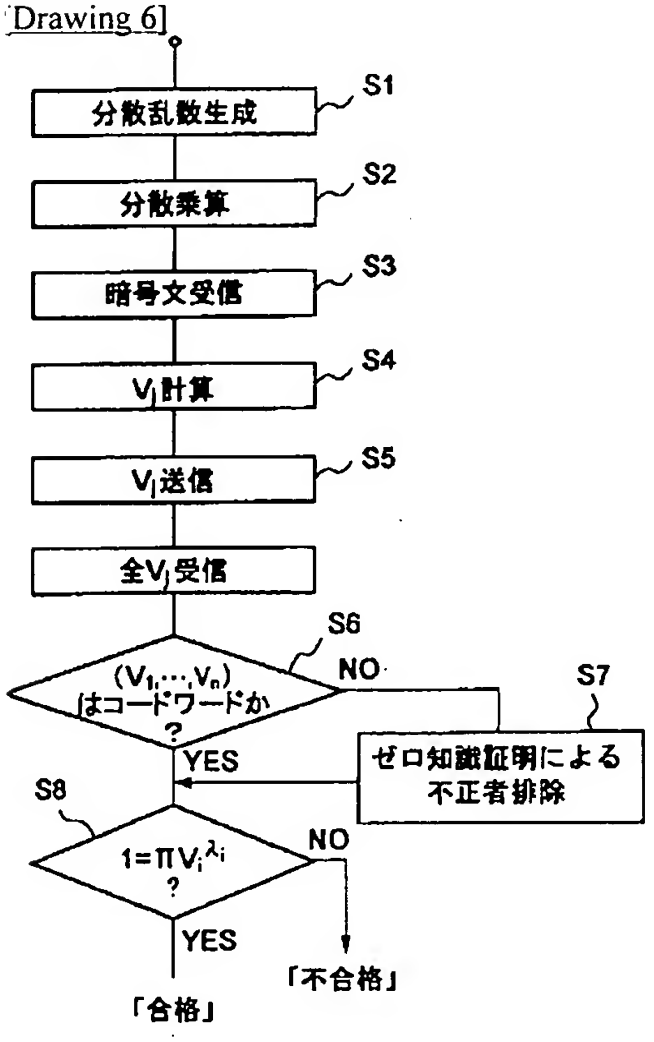

図 6

[Drawing 7]

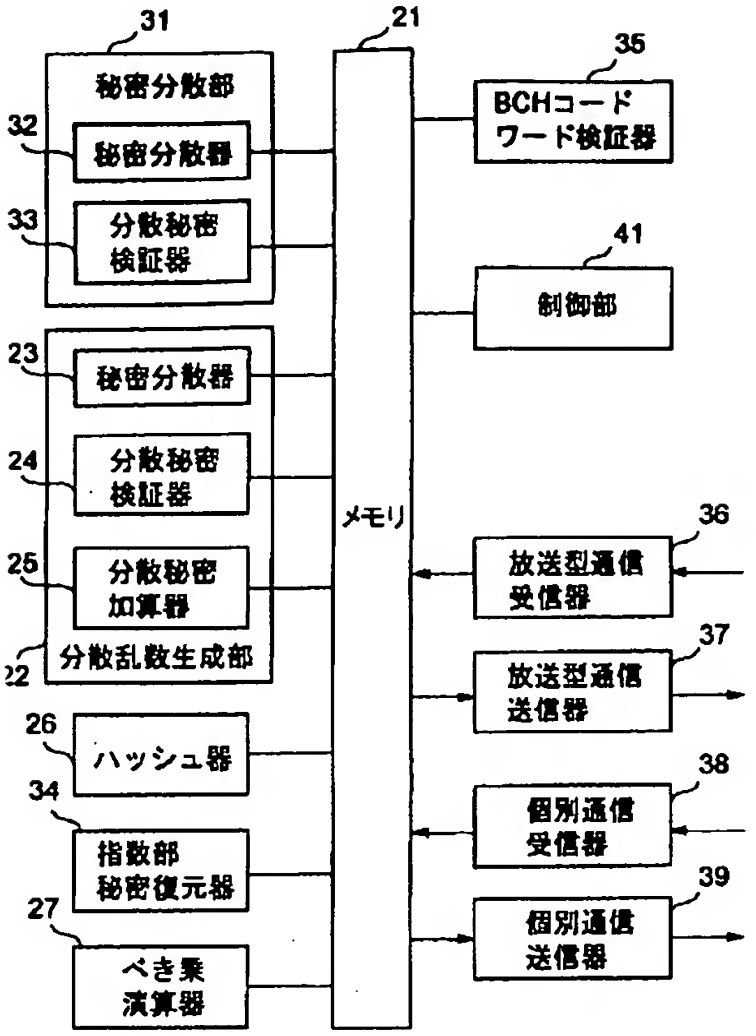

図 7

[Drawing 8]

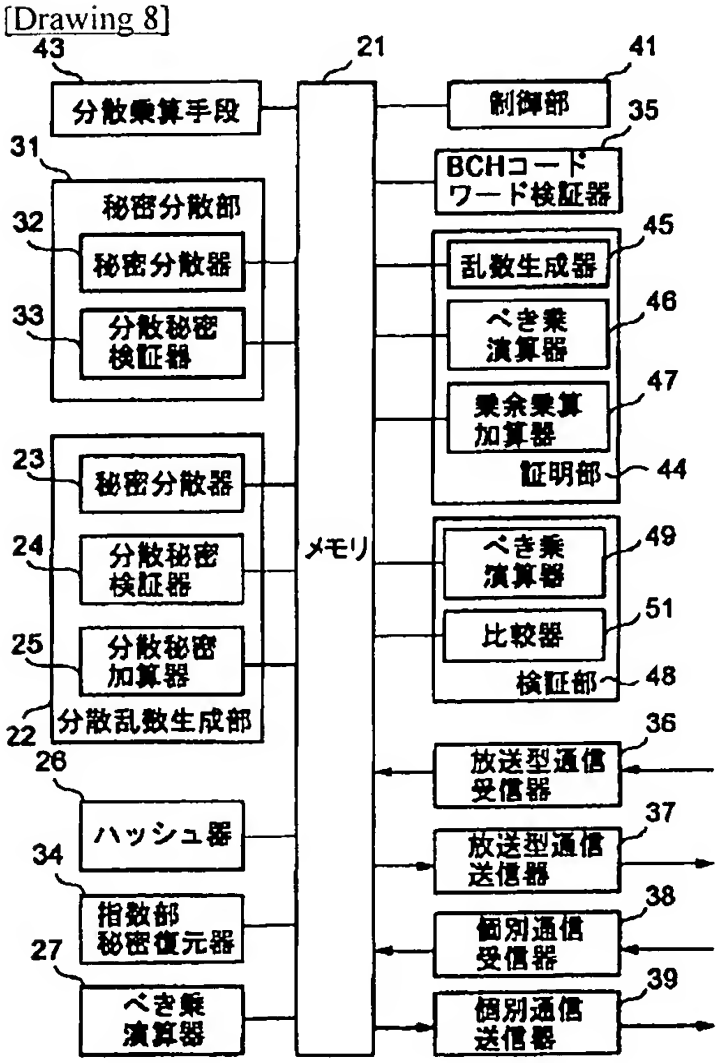

図 8

Translation done.]